Final Technical Report

Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy – Phase 2

ISRN L3COM/HENSCHEL/TR -- 2009/001

Contract Number: N00014-07-C-0832

Prepared For

Office of Naval Research

Prepared by:

L3 communications
Henschel
9 Malcolm Hoyt Drive
Newburyport, MA 01950 USA

This page intentionally left blank.

Intelligent Advanced Communications IP Telephony
Feasibility for the U.S. Navy – Phase 2

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**		
1. REPORT DATE *(DD-MM-YYYY)* 03-31-2009	**2. REPORT TYPE** Research	**3. DATES COVERED** *(From - To)* 09-17-2007 – 03-31-2009
4. **TITLE AND SUBTITLE** Intelligent Advanced Communications Phase 2, Research and Conceptual Design		**5a. CONTRACT NUMBER** N00014-07-C-0832 **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6**. AUTHOR(S)** Binns, Todd D; Principle Investigator Weaver, Joseph D.: Investigator		**5d. PROJECT NUMBER** N.A. **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Henschel Inc., L-3 Communications 9 Malcolm Hoyt Drive Newburyport, MA 01950-4017		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Naval Research 875 N Randolph St., Suite 1425 Arlington, VA 22203-1995		**10. SPONSOR/MONITOR'S ACRONYM(S)** ONR **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited		
13. SUPPLEMENTARY NOTES		

Intelligent Advanced Communications IP Telephony
Feasibility for the U.S Navy – Phase 2

14. ABSTRACT

The objective of this research paper and the Proof-of-Concept IP Communications Terminal is to research technologies and solutions supporting the communications infrastructure necessary to implement a unified VoIP (IP telephony), Video, and Data infrastructure on US Navy vessels.

This report is based on the following research and validation testing:

- L-3 Henschel internal research,
- L-3 Henschel VoIP lab research,
- L-3 Henschel prototyping of a VoIP Communications Terminal,
- Unified Capabilities Requirements 2008,
- Government documents focusing on network security and implementation, and
- The L-3 Henschel Technical Report *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy*, Volumes 1 and 2 (ISRN L3COM/HENSCHEL/TR-2007/001).

The major findings for implementing an integrated VoIP (IP telephony), Video, and Data infrastructure on US Navy vessels are:

- Different network data can be unified onto the same IP network and separated into virtual networks,
- The Proof-of-Concept IP Communications Terminal can handle calls as well as other network tasks, bringing communications and data together into a unified device,
- Assured Services Session Initiated Protocol (AS-SIP) can be implemented on an end device,
- Implementing an IP solution on US Navy vessels is feasible and achievable,
- There will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COTs (Commercial-Off-The-Shelf) products,
- The US Government is assessing the benefits of Open-Source versus proprietary vendor offerings, and
- The unification of VoIP (IP telephony), Video, and Data will be secure as detailed in US Department of Defense publications.

15. SUBJECT TERMS
VoIP, SIP, H.323, US Navy, Vessels, Communications, Network, SVoIP, VoSIP, SVoSIP, AS-SIP, Assured Services SIP

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Christopher P. Rigano (CISSP)
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	224	**19b. TELEPHONE NUMBER** *(include area code)* 703.696.5942

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Intelligent Advanced Communications IP Telephony
Feasibility for the U.S. Navy – Phase 2

Abstract

The objective of this research paper and the Proof-of-Concept IP Communications Terminal is to research technologies and solutions supporting the communications infrastructure necessary to implement a unified VoIP (IP telephony), Video, and Data infrastructure on US Navy vessels.

This report is based on the following research and validation testing:

- L-3 Henschel internal research,
- L-3 Henschel VoIP lab research,
- L-3 Henschel prototyping of a VoIP Communications Terminal,
- Unified Capabilities Requirements 2008,
- Government documents focusing on network security and implementation, and
- The L-3 Henschel Technical Report *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy*, Volumes 1 and 2 (ISRN L3COM/HENSCHEL/TR-2007/001).

The major findings for implementing an integrated VoIP (IP telephony), Video, and Data infrastructure on US Navy vessels are:

- Different network data can be unified onto the same IP network and separated into virtual networks,
- The Proof-of-Concept IP Communications Terminal can handle calls as well as other network tasks, bringing communications and data together into a unified device,
- Assured Services Session Initiation Protocol (AS-SIP) can be implemented on an end device,
- Implementing an IP solution on US Navy vessels is feasible and achievable,
- There will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COTs (Commercial-Off-The-Shelf) products,
- The US Government is assessing the benefits of Open-Source versus proprietary vendor offerings, and
- The unification of VoIP (IP telephony), Video, and Data will be secure as detailed in US Department of Defense publications.

This page intentionally left blank.

Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy – Phase 2

Table of Contents

Paragraph	Title	Page
Abstract		v
CHAPTER 1	EXECUTIVE SUMMARY	1
1.1	Objectives	1
1.1.1	Introduction	1
1.1.2	Proof-of-Concept	2
1.1.3	Research and Implementation	3
1.1.4	Physical Network Research	4
1.1.5	Phase 3 Recommendations	5
1.1.6	Conclusion	7
CHAPTER 2	iACT AS-SIP END INSTRUMENT	9
2.1	iACT AS-SIP End Device Overview	9
2.1.1	L3_AS_SIP_Phone Installation	9
2.1.1.1	L3_AS_SIP_Phone Configuration	10
2.1.1.2	Configuration Parameters	10
2.1.2	L3_AS_SIP_Phone Usage	11
2.1.2.1	Starting L3_AS_SIP_Phone	11
2.1.2.2	Exiting L3_AS_SIP_Phone	11
2.1.2.3	Phone Screens	11
2.1.2.4	Preset Modes	12
2.1.2.5	Placing Calls	12
2.1.2.6	Dial Pad Mode	13
2.1.2.7	Placing Calls	13
2.1.3	Configuration	14
2.1.3.1	Configure Speed Dials	15
2.1.3.2	Speed Dials Dialogue Box	15
2.1.4	Diagnostics	16
2.1.5	Telephony Functions	17
2.1.5.1	Answering Calls	17
2.1.5.2	Call/Hangup	17
2.1.5.3	Hold/Resume	18
2.1.5.4	Forward Enable/Disable	18
2.1.5.5	Transfer	18
2.1.5.6	Redial	19
2.1.6	Resource Priority	19
2.1.6.1	Precedence Domain	19

Table of Contents - Continued

Paragraph	Title	Page
2.1.6.2	L3_AS_SIP_Phone Interoperability Tests	20
2.1.7	Button and Menu Settings	20
2.1.7.1	Button Settings	20
2.1.7.2	Menu Settings	21
2.1.8	Conclusion	22
2.2	Hardware Development	23
2.2.1	Hardware Selection	23
2.2.1.1	Processor	23
2.2.1.2	Hard Drive	24
2.2.1.3	Sound Cards	25
2.2.1.4	Power Supply	26
2.2.1.5	Display Head	26
2.2.2	Packaging of Hardware	27
2.2.2.1	Processor Heat Dissipation	27
2.2.2.2	Reduced Size	27
2.2.3	Performance Benchmarks	28
2.2.4	Conclusion	32
CHAPTER 3	iACT AS-SIP IP COMMUNICATIONS TERMINAL RESEARCH	33
3.1	Introduction	33
3.1.1	Proof-of-Concept: Architecture, Design and Implementation Details	33
3.1.1.1	L3_AS_SIP_Phone.cs	34
3.1.1.2	ASIP_GUI.cs	34
3.1.1.3	ASIP_GUIDesigner.cs	34
3.1.1.4	ASIP_PcapSettingsConfig.cs	34
3.1.1.5	ASIP_PcapSettingsConfig.Designer.cs	34
3.1.1.6	ASIP_SipSettingsConfig.cs	35
3.1.1.7	ASIP_SipSettingsConfig.Designer.cs	35
3.1.1.8	ASIP_SpeedDialConfig.cs	35
3.1.1.9	ASIP_SpeedDialConfig.Designer.cs	35
3.1.1.10	ASIP_SplashScreen.cs	35
3.1.1.11	ASIP_SplashScreen.Designer.cs	35
3.1.1.12	L3_AS_SIP_Phone – Code	36
3.1.1.12.1	Init – Splash Screen	36
3.1.1.12.2	SIP Setting	37
3.1.1.12.3	SpeedDialConfig	37
3.1.1.12.4	Pcap Settings	38
3.1.1.12.5	ASIP_GUI	39

Table of Contents - Continued

Paragraph	Title	Page
3.1.2	Proof-of-Concept Software Development	47
3.1.2.1	Design Platform Decisions	47
3.1.2.2	Design Platform Options	47
3.1.3	Proof-of-Concept: Development Environment	48
3.1.4	Proof-of-Concept: Building AS-SIP Code	49
3.1.5	Proof-of-Concept: Running Code Locally	51
3.1.6	Proof-of-Concept: Installing Proof-of-Concept Hardware	51
3.1.7	Proof-of-Concept Security	52
3.1.7.1	Device Access Security	52
3.1.7.2	Session Access Security	53
3.1.7.3	Classified/Unclassified Network Security	53
3.1.7.4	Remote Device Management	53
3.1.7.5	General VoIP Security Recommendations	54
3.1.7.6	Transport Layer Security	54
3.1.7.7	Secure Real-time Transport Protocol	55
3.1.8	Proof-of-Concept Assured Services SIP: An End Device Perspective	56
3.1.8.1	Reasons for AS-SIP	56
3.1.8.2	AS-SIP Signaling – Multilevel Precedence and Preemption	57
3.1.9	SIP RFCs & Unified Capabilities Requirements 2008 (UCR 2008)	59
3.1.9.1	Proof-of-Concept: Supported RFCs	59
3.1.9.2	RFCs of Importance	59
3.1.9.3	AS-SIP Areas of Concern	63
3.2	PoC IP Communications Terminal: Configuration and Usage	64
3.2.1	Basic Configuration	64
3.2.1.1	Basic Configuration Procedure	65
3.2.1.2	Setting Speed Dials	68
3.2.2	Using the L3_AS_SIP_Phone	70
3.2.2.1	Preset Modes	71
3.2.2.2	Dial Pad Mode	71
3.2.3	Diagnostics	72
3.2.3.1	Call Functions	73
3.2.3.2	Call/Hangup	73
3.2.3.3	Hold/Resume	74
3.2.3.4	Forward Enable/Disable	74
3.2.3.5	Transfer	74
3.2.3.6	Redial	75
3.2.4	Resource Priority	75
3.2.5	Precedence Domain	75
3.2.6	Configuring L3_AS_SIP_Phone Menus and Buttons	76

Table of Contents - Continued

Paragraph	Title	Page
3.2.6.1	Configuring Button Settings	77
3.2.6.2	Menu Settings	79
3.2.7	L3_AS_SIP_Phone Interoperability Tests	80
CHAPTER 4	PHYSICAL NETWORK FEASIBILITY	81
4.1	Introduction	81
4.1.1	Scope	81
4.1.2	iACT VoIP Network Physical Connectivity	81
4.1.2.1	Full Mesh	81
4.1.2.2	Partial Mesh	82
4.1.2.3	Dual-Redundant Mesh Network	82
4.1.3	iACT Network Topology	82
4.1.3.1	Overview	82
4.1.3.2	Gigabit Ethernet Physical Connections	84
4.1.3.3	End-User Devices	84
4.1.3.4	Servers and Appliances	85
4.1.4	VLANs for Converged Voice, Video and Data	85
4.1.4.1	Spanning Tree Protocol (STP)	86
4.1.4.2	Rapid Spanning Tree Protocol (RSTP)	87
4.1.4.3	Multiple Spanning Tree Protocol (MSTP)	88
4.1.5	Dual-Homing Vital Components	89
4.1.6	Subnetting	89
4.1.6.1	Single Subnet	90
4.1.6.2	Multiple Subnets	90
4.1.7	Routing Protocols	90
4.1.7.1	Routing Information Protocol (RIP)	90
4.1.7.2	Open Shortest Path First (OSPF)	90
4.1.7.3	Border Gateway Protocol (BGP)	91
4.1.8	Quality of Service	91
4.1.8.1	Overview	91
4.1.8.2	Mean Opinion Score/Perceptual Evaluation of Speech Quality	92
4.1.8.3	Latency, Jitter, and Packet Loss	93
4.1.8.3.1	Latency	93
4.1.8.3.2	Jitter	93
4.1.8.3.3	Packet Loss	94
4.1.9	Priority Queuing	94
4.1.9.1	Ethernet Packet Header Priority	94
4.1.9.2	IP Header DiffServ	95
4.1.9.3	Real-time Transport Protocol	96

Table of Contents - Continued

Paragraph	Title	Page
4.1.10	Network Address Translation	96
4.1.10.1	Impact of NAT on SIP and RTP Session Border Controller	96
4.1.10.2	The RTP answer	97
4.1.11	Security	97
4.1.11.1	IPSEC Delays Session/Call Establishment	97
4.1.11.2	Transport Layer Security (TLS)	98
4.1.11.3	Secure Sockets Layer (SSL)	99
4.1.12	IP Multicasting	99
4.1.13	Test Results	101
4.1.13.1	Voice Quality Test Description Test Files	101
4.1.13.2	Test Conditions	101
4.1.13.3	Voice Quality Test Setup	102
4.1.13.4	Test Condition 1 (Baseline)	102
4.1.13.4.1	MOS/PESQ	103
4.1.13.4.2	Average Jitter	105
4.1.13.5	Test Condition 2 (VLANs)	108
4.1.13.6	Test Condition 3 (QoS)	109
4.1.13.7	Test Condition 4 (File Transfer Data)	111
4.1.13.8	Switch Performance	112
4.1.14	Test Result Summary	112
4.1.14.1	Observation 1 (Results versus Voice Gender)	112
4.1.14.2	Observation 2 (VLAN’s versus Baseline)	113
4.1.15	Conclusion	113
4.2	Feasibility of Using Open System and Non-Proprietary Protocols	115
4.2.1	Introduction	115
4.2.2	Session Initiation Protocol	115
4.2.3	Current Supported Features	117
4.2.4	Shortcomings of SIP	119
4.2.5	Assured Services SIP	120
4.2.6	Shortcomings of AS-SIP	120
4.2.7	Trunks Verses End Devices	120
4.2.8	Open Source	121
4.2.9	Conclusion	121
4.3	Feasibility of Wireless Phones	122
4.3.1	Introduction	122
4.3.1.1	Set Up of the Wireless Network	122
4.3.1.2	Security of the Wireless Network	123

Table of Contents - Continued

Paragraph	Title	Page
4.3.1.3	Set Up of VoIP on the Wireless Network	123
4.3.1.4	Ascom and Aruba Equipment	123
4.3.1.5	Ascom Portable Device Manager	124
4.3.1.6	Ascom Integrated Message Server	124
4.3.1.7	Phones	125
4.3.1.8	Ascom Phone Setup	125
4.3.2	Wireless in a "Tin Can"	126
4.3.2.1	Bandwidth and Access Points	128
4.3.2.2	Wi-Fi vs. WIFCOM	130
4.3.3	Conclusion	131
4.4	Feasibility of Reliability and Maintainability	132
4.4.1	Introduction	132
4.4.2	Network Challenges	132
4.4.3	Dual-Redundant Mesh Network	133
4.4.4	Media Gateways	135
4.4.4.1	SmartLink Micro –ATA Evaluation	136
4.4.4.2	Multitech MultiVoIP Evaluation	137
4.4.4.3	SIPx Server Evaluation	138
4.4.4.5	Additional Considerations	138
4.4.4.6	Conclusion	139
4.4.5	Unified Capabilities Requirements 2008 (UCR2008)	139
4.4.6	Conclusion	142
4.5	Feasibility of IP-Announcing	143
4.5.1	Introduction	143
4.5.1.1	IP Announcing and Commercial-Off-the-Shelf (COTS) Systems	143
4.5.1.2	Latency and IP Announcing	146
4.5.1.3	Hybrid Announcing Design	146
4.5.2	IP Announcing Shortcomings	148
4.5.3	Conclusion	149
CHAPTER 5	RECOMMENDATIONS AND CONCLUSION	151
5.1	Introduction	151
5.1.1	Recommendation	151
5.1.2	Conclusion	152

Table of Contents - Continued

Paragraph **Title** **Page**

REFERENCES 153

APPENDIX A iACT MEAN OPINION SCORE PROCEDURES 159

A.1 Test Setup 161

A.2 Calibration 161
A.2.1 Initial State 161
A.2.2 Establish Voice Connection 162
A.2.3 Calibrate Audio Signals 162

A.3 MOS (Mean Opinion Score) Evaluation 168
A.3.1 Voice Transmission/Reception 169
A.3.2 FTU (File Transfer Utility) 170
A.3.3 Data Analysis (VQT) 174
A.3.4 Data Viewing (VQTNetViewer) 177

A.4 RTD (Round Trip Delay) 179

APPENDIX B L3_AS_SIP_PHONE INTEROPERABILITY TESTS 183

B.1 L3_AS_SIP_Phone Interoperability Tests 185
B.1.1 Test 1: Place Outgoing Call Resource Priority Set to Routine 185
B.1.2 Test 2: Place Outgoing Call Resource Priority Set to Priority 185
B.1.3 Test 3: Place Outgoing Call Resource Priority Set to Immediate 186
B.1.4 Test 4: Place Outgoing Call Resource Priority Set to Flash 186
B.1.5 Test 5: Place Outgoing Call Resource Priority Set to Flash-Override 186
B.1.6 Test 7: Receive Incoming Call Resource Priority Set to Routine 187
B.1.7 Test 8: Receive Incoming Call Resource Priority Set to Priority 187
B.1.8 Test 9: Receive Incoming Call Resource Priority Set to Immediate 188
B.1.9 Test 10: Receive Incoming Call Resource Priority Set to Flash 188
B.1.10 Test 11: Receive Incoming Call Resource Priority Set to Flash-Override 189
B.1.11 Test 13: Call Forward Test 189
B.1.12 Test 15: Call Transfer Test 189
B.1.13 Test 16: Call Hold Test 190

SYMBOLS, ABBREVIATIONS, AND ACRONYMS 191

This page intentionally left blank.

List of Illustrations

Figure	Title	Page
Figure 1-1	Proof-of-Concept	3
Figure 1-2	Base Network Design	4
Figure 1-3	Network with VLANs Added	5
Figure 1-4	Hybrid Communications Terminal Block Diagram	6
Figure 2-1	L3_AS_SIP XML Configuration File	11
Figure 2-2	L3_AS_SIP_Phone GUI Sample Preset Menu	13
Figure 2-3	L3_AS_SIP_Phone GUI Sample Dial Pad Menu	14
Figure 2-4	L3_AS_SIP_Phone GUI Configuration Menu	15
Figure 2-5	Speed Dial Configuration Dialogue Box	16
Figure 2-6	On-Screen Keyboard Window	16
Figure 2-7	Diagnostics Screen	17
Figure 2-8	L3 AS-SIP Phone Resource Priority Protocol Trace	20
Figure 2-9	L3 AS-SIP Phone Button Configuration XML	21
Figure 2-10	L3 AS-SIP Menus Configuration XML	22
Figure 2-11	MPL-10	24
Figure 2-12	Imation Solid State Drive	25
Figure 2-13	Proof-of-Concept	27
Figure 2-14	Completed Proof-of-Concept	28
Figure 2-15	Hard Disk Benchmark	29
Figure 2-16	Processor Benchmark	30
Figure 2-17	Memory Benchmark	30
Figure 2-18	Display Adapter Benchmark	31
Figure 3-1	Init - Splash Screen	36
Figure 3-2	SIP Settings	37
Figure 3-3	Setting Speed Dial Configuration	38
Figure 3-4	Pcap Settings	39
Figure 3-5	ASIP_GUI (Sheet 1 of 7)	40
Figure 3-6	L3_AS_SIP Development Directory	49
Figure 3-7	GUI Directory	50
Figure 3-8	Microsoft Visual Studio	51
Figure 3-9	L-3_AS-SIP Directory	52
Figure 3-10	TLS Protocol Handshake (Reprinted from RFC 5246)	55
Figure 3-11	Secure Real-time Transport Protocol (SRTP)	56
Figure 3-12	Disconnect Message Cause Values	58
Figure 3-13	Codepoints for Signal Values	58
Figure 3-14	SIP Core Signaling	60

List of Illustrations - Continued

Figure	Title	Page
Figure 3-15	Resource Priorities Protocol Trace	61
Figure 3-16	Proof-of-Concept Configuration Menu	65
Figure 3-17	Configure Speed Dials Button on the Configuration Menu	68
Figure 3-18	L3_AS-SIP_Phone GUI Sample Preset Menu	71
Figure 3-19	L3_AS_SIP_Phone GUI Sample Dial Pad Menu	72
Figure 3-20	Diagnostic Menu Screen	73
Figure 3-21	L3_AS_SIP_Phone Resource Priority Protocol Trace	76
Figure 3-22	Configuration File for L3_AS_SIP_Phone XML	77
Figure 3-23	Button Speed Dial Settings	78
Figure 3-24	L3 AS-SIP Phone Button Configuration XML	79
Figure 3-25	L3 AS-SIP Menus Configuration XML	80
Figure 4-1	Switch Layout	83
Figure 4-2	Test Bed Layout (Main Cabinet)	84
Figure 4-3	iACT VLAN Map	86
Figure 4-4	MAC Header (Layer 2)	95
Figure 4-5	MAC Header Layer with Tag	95
Figure 4-6	iACT Voice Quality Test Setup	102
Figure 4-7	PESQ Score (Voice Only)	103
Figure 4-8	PESQ Score (Voice and Navigational Data)	104
Figure 4-9	PESQ Score (Voice, Navigational, and Video Data)	104
Figure 4-10	PESQ Score (Voice, Navigational, Video Data, and File Transfer Data)	105
Figure 4-11	Average Jitter (Voice Only)	106
Figure 4-12	Average Jitter (Voice and Navigational Data)	106
Figure 4-13	Average Jitter (Voice, Navigational, and Video Data)	107
Figure 4-14	Average Jitter (Voice, Navigational, Video, and File Transfer Data)	107
Figure 4-15	PESQ Score with VLANs	108
Figure 4-16	Average Jitter with VLANs	109
Figure 4-17	PESQ Scores with QoS and VLANs	110
Figure 4-18	PESQ Scores with QoS and VLANs	111
Figure 4-19	PESQ with QoS, VLANs and File Transfers	111
Figure 4-20	Average Jitter with VLANs and File Transfers	112
Figure 4-21	Aruba Network with MC-200	124
Figure 4-22	PDM Configuration Screen for Device Settings	126
Figure 4-23	Distributed System with RF Management	127
Figure 4-24	Wireshark SIP Call Between Ascom Phones	128
Figure 4-25	Wireshark SIP Call Details Between Ascom Phone	129
Figure 4-26	Aruba MC-200 SIP Call Between Ascom Phones	129

List of Illustrations - Continued

Figure **Title** **Page**

Figure 4-27 Summary of SIP Call at MC-200 Port ... 130
Figure 4-28 Control Systems Operation Over DMS ... 134
Figure 4-29 Patton-MATA-Error.pcap Window ... 136
Figure 4-30 Patton SmartLink – ATA Window ... 137
Figure 4-31 Avaya G700 Media Gateway (Front View) ... 138
Figure 4-32 COTS Announcing System ... 145
Figure 4-33 Hybrid Announcing System ... 148
Figure A-1 Test Setup ... 161
Figure A-2 VQuad Main Window ... 163
Figure A-3 Sound Device Association Window (Laptop 3) ... 163
Figure A-4 VQuad Screens ... 169
Figure A-5 Running Script Screens ... 170
Figure A-6 FTU Program ... 171
Figure A-7 FTU Load Configurations Window ... 171
Figure A-8 FTU Window ... 172
Figure A-9 FTU File Copy Running ... 173
Figure A-10 VQT Window ... 174
Figure A-11 VQT Auto Measurement Window ... 174
Figure A-12 VQT Configuration Files Screen ... 175
Figure A-13 VQT Auto Measurement Files Window ... 175
Figure A-14 GL Voice Quality Test Window ... 176
Figure A-15 VQTNetViewer Screen ... 177
Figure A-16 VQTNetViewer Window ... 178
Figure A-17 VQTNetViewer Data Display Window ... 179
Figure A-18 RTD Main Window ... 180
Figure A-19 RTD Running Window ... 181

List of Tables

Table **Title** **Page**

Table 2-1 L3_AS_SIP XML 10
Table 2-2 Resource Priority Decimal Values 19
Table 2-3 Hard Drive Raw Test Data 31
Table 3-1 Resource Priority Decimal Values 61
Table 3-2 Additional Configuration Menu Buttons 67
Table 3-3 Resource Priority Decimal Values 75
Table 4-1 End-User Devices 85
Table 4-2 Servers and Appliances 85
Table 4-3 iACT VLANs 85
Table 4-4 Switch Performance Chart (1 hr Average) 112
Table 4-5 Baseline Results versus Voice Gender 113
Table 4-6 VLANs versus Baseline 113
Table 4-7 Features Supported in Sphericall IP PBX Release 5 117
Table 4-8 Zone Configuration 145

CHAPTER 1 EXECUTIVE SUMMARY

1.1 Objectives

The objective of this research paper and the Proof-of-Concept IP Communications Terminal is to research technologies and solutions supporting the communications infrastructure necessary to implement a unified VoIP (IP telephony), Video and Data infrastructure on US Naval vessels.

This report is based on the following research and validation testing:

- L-3 Henschel internal research
- L-3 Henschel VoIP lab research
- L-3 Henschel prototyping of a VoIP Communications Terminal
- Unified Capabilities Requirements, 2008
- Government documents focusing on network security and implementation.
- L-3 Henschel *Intelligent Advanced Communications IP Feasibility for the U.S. Navy, Volumes 1 and 2* (ISRN L3COM\HENSCHEL\TR-2007\001).

1.1.1 Introduction

This document is separated into five chapters: Chapter 1 includes the Abstract and the Executive Summary. Chapter 2 contains detailed information on the Proof-of-Concept (PoC) VoIP communications terminal. Chapter 3 contains information on the Communications Terminal research. Chapter 4 contains the physical network feasibility study investigation conclusions, and Chapter 5 contains Phase 3 recommendations and the conclusion. Appendix A and Appendix B comprise supporting information and a DVD that contains the source code to the PoC not covered under the Telesoft International and Global IP agreement (including the abstraction layer that isolated the calls to Telesoft International proprietary interface), as well as this report.

The feasibility study and PoC investigation have resulted in these lessons learned about VoIP:

- **The network is the critical piece –** If the network is not configured and sized for current and future requirements, the Mean Opinion Score (MOS) will not be acceptable.

- **The US Navy needs reliability over technology –** The tactical functions must be assiduous and available at all times.

- **VoIP has become mission critical –** VoIP is being used commercially, in the telephone backbone, and on military bases around the world. It has been approved by several military organizations including JITC.

- **Planning and testing up front is critical –** Understanding and getting every owner of data on the network; the need to work together to develop the plan for QoS and reliability for the complete network.

From the investigation and lessons learned these are the major findings for implementing a unified VoIP (IP telephony), Video and Data infrastructure on naval vessels:

- Different network data can be integrated on to the same IP network and separated into virtual networks.
- The Proof-of-Concept IP Communications Terminal can handle calls as well as other network tasks bringing together communications and data into a unified device.
- Assured Services Session Initiated Protocol (AS-SIP) can be implemented on a unified device.
- Implementing an IP solution on US Navy vessels is feasible and achievable.
- There will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COTs products.
- The government is assessing the benefits of Open Source versus proprietary vendor offerings.
- The unification of VoIP (IP telephony), Video and Data can be secure as detailed in US Department of Defense publications.

1.1.2 Proof-of-Concept

The Proof-of-Concept (PoC) (Figure 1-1) is a next generation prototype of a Basic Rate Interface (BRI) communication terminal that is employed on several vessels in the fleet. The design is reduced in height from the current communications terminal, but its footprint is the same. The project changed at the end 2008; as Avaya was not able to support AS-SIP unified devices on Trident Warrior 2009, so the PoC could not be tested during the Trident Warrior trial. Plans were put together to test with other manufactures of AS-SIP devices since no US Navy lab was found to be configured for testing of a unified device that supported AS-SIP.

Figure 1-1 Proof-of-Concept

The IP Telephony Services within the PoC are based on AS-SIP, Session Description Protocol (SDP), and Real-time Protocol (RTP/RTCP) and provide precedence and preemption functionality in accordance with the AS-SIP specification. The PoC is a software-hardware solution that runs on Microsoft Windows XP embedded (XPe), and provides telephony features and Assured Services on a 5 in. x 4 in. touch screen device. It is designed for configurable constraints on resource priorities and precedence domains with support for preemption tones and response codes as defined in the AS-SIP specification.

1.1.3 Research and Implementation

Contained in Chapter 2 is a summary of research and implementation findings for iACT Phase 2 PoC software development.

- A description of the PoC software architecture, design and implementation details
- A description of the PoC software development environment, build environment, and installation
- A description of the PoC software security
- A description of development platform options and decisions
- A description of the functional usage of the PoC
- An overview of Assured Services SIP from an end device perspective

The PoC is to prove the ability of SIP to be used on board a US Navy vessel. It was designed to exercise the telephony functionalities that are required of an IP

communications terminal. Its focus is to test telephony functionality and graphical user interface (GUI) designs. The design was done around Telesoft International, Inc (Telesoft) stacks and the Global IP Sound (GIPS) Voice Engine. These third party software products reduced the time of development, since they are the core telephony and media stream components. They allow any company to implement the same source code by purchasing rights from the individual companies, or add their own technology if desired.

1.1.4 Physical Network Research

The need for the Total Ship Computing Environment (TSCE) must be reliable and maintainable by the sailors on the vessels. This includes both tactical and administrative networks, including communications. The network infrastructure is the paramount part of the complete system (Figure 1-2). If the network is not engineered to support the requirements of the unified devices that will be connected to it, the reliability will never be achieved. Only after the network has been designed for reliability will it be possible to achieve maintainability. With current topologies of segregated networks, migrating to the PMW-160/ C4I Consolidated Afloat Networks and Enterprise Services (CANES) direction of integrating all the requirements into a single network, design is critical to the network's ability to handle the traffic and limit jitter and packet loss.

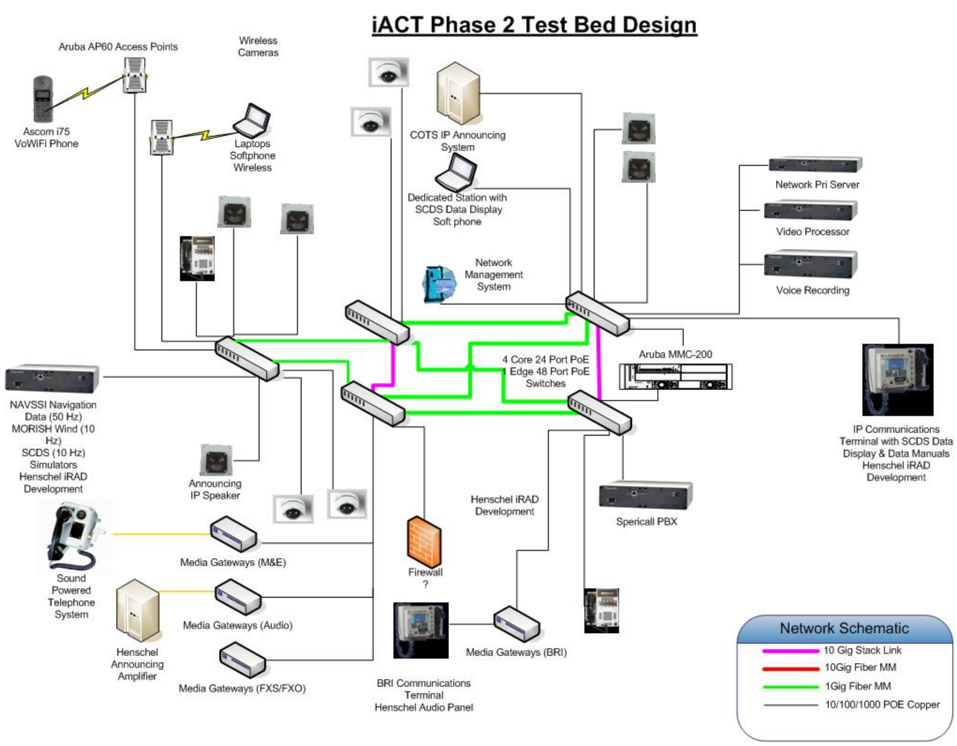


Figure 1-2 Base Network Design

After the network is designed correctly, then the protocols that run on that network need to be engineered accordingly to prevent "denial of access" and/or traffic issues caused by

interactions, or bad code in the individual or in unison with other protocols. This also relates to the end devices; be it a computer, IP telephone or a bar code scanner, they all need to be engineered into the network to extend the network's reliability. To protect different functions on the network it is divided into VLANs (Figure 1-3). This limits network traffic that can affect the whole network, to only what is located on its own VLAN.

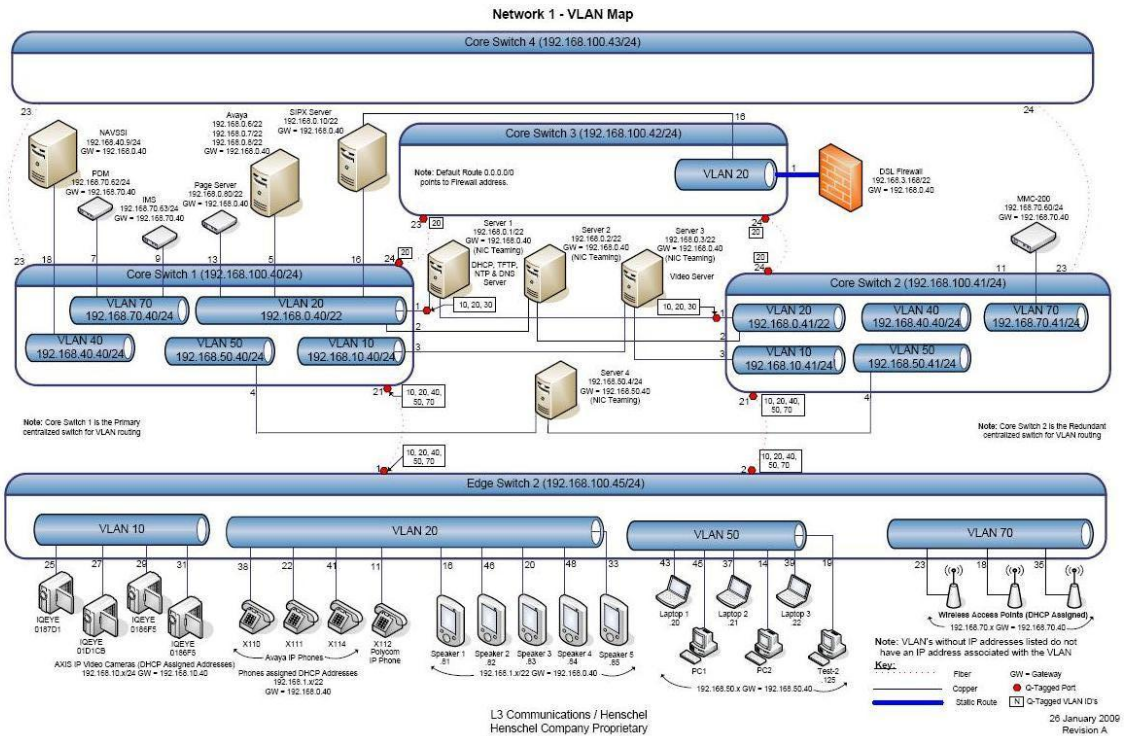


Figure 1-3 Network with VLANs Added

Internal communications on a vessel afloat is critical. The ability for sailors to be mobile and still have the same connectivity as if at a stationary phone is also critical. In Phase 1, several different technologies were evaluated and WiFi was noted as the best overall solution. We implemented a WiFi network built around Aruba network components and Ascom WiFi phones.

Announcing is a critical part of internal communications; it is used for both general announcements and for critical information distribution. The flight deck of an aircraft carrier is a major user of announcing and constitutes a challenging environment for broadcasting sound. IP Announcing utilizes the IP network infrastructure to carry the announcements, instead of dedicated cable runs.

1.1.5 Phase 3 Recommendations

The objective of Phase 3 is to take the information from the Phase 2 testing and PoC and the information compiled in Phase 1, and create a working Proof-of-Concept so that

different groups in the Armed Forces can evaluate the technology of an IP Communications Terminal that is a hybrid with a BRI capability added to the Phase 2 PoC. The deliverable will be the Hybrid PoC (HPoC) (Figure 1-4) and its related documentation, and the methods used to implement the two technologies to work in unison. The telephony module will combine the two technologies and present them as a single interface to the GUI/Application developer. The GUI/application will represent the features that are required for a sailor to test the functions required to determine if the technology is ready for shipboard implementation. This will include but is not limited to speed dials, numeric dial pad, and selection of type of call. It will not expose features that are for ease of configuration or ability to switch between multiple profiles. HPoC will be housed in an IVUT to allow for the size of the BRI ISDN card, if required. Even though other technologies are made available by connection to the network, a limited exploration of them will be done during this phase and will be left for future productization.

Proof of Concept

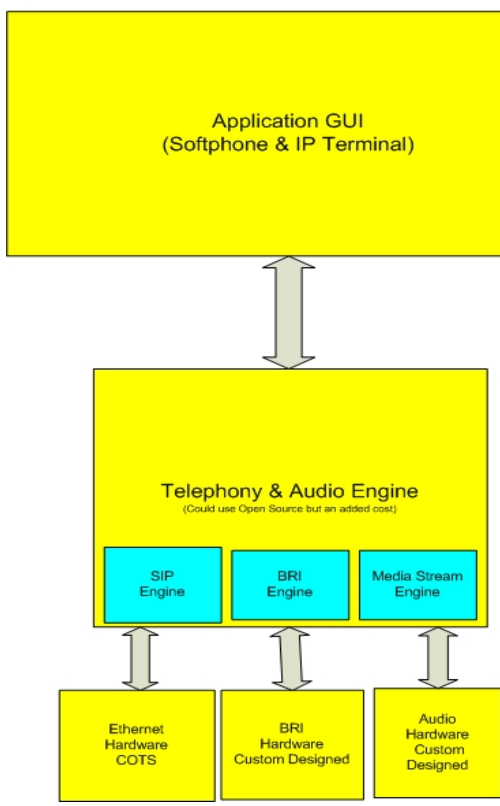


Figure 1-4 Hybrid Communications Terminal Block Diagram

1.1.6 Conclusion

The key points of this research paper and creation of the Proof-of-Concept IP Communications Terminal for implementing a unified VoIP (IP telephony), Video and Data infrastructure on naval vessels are summarized below:

1. Implementing a unified VoIP (IP telephony), Video and Data infrastructure is becoming pervasive in land bases.
2. Implementing a unified VoIP (IP telephony), Video and Data infrastructure for US Navy vessels is feasible and achievable. Due to the unique requirements of the US Navy, there is a staged implementation planned from feasibility to Proof-of-Concept, followed by evaluation in a US Navy lab and US Navy ship.
3. There is and will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COTs products.
4. Assured Services SIP brings to VoIP what multi-level precedence and preemption brought to the current communication network.
5. The unification of VoIP (IP telephony), Video and Data will be secure as detailed by US Department of Defense publications.

This page intentionally left blank.

CHAPTER 2 iACT AS-SIP END INSTRUMENT

2.1 iACT AS-SIP End Device Overview

This document describes the configuration, operation, and plan for early-stage interoperability testing of the Proof-of-Concept (PoC) end instrument being developed at L-3 Communications-Henschel. The project, titled *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy - Phase 2*, is being developed for the Office of Naval Research (ONR) on the feasibility of VoIP on Navy vessels.

In Phase 2 of this study Proof-of-Concept end instrument is being developed with a Commercial-Off-the-Shelf (COTS) SIP stack and voice engine modified to support Assured Services SIP (AS-SIP) with the call features needed, and the enhancements desired for Navy vessels. The objective is to demonstrate the feasibility for IP Telephony to provide enhanced functionality to the existing telephony and announcement services over converged network architecture with data, multimedia, and telephony traffic.

The IP Telephony Services will be based on Assured Services SIP (AS-SIP), Session Initiation Protocol (SIP), Session Description Protocol (SDP), and Real-time Protocol (RTP/RTCP). The end instrument will provide precedence and preemption functionality in accordance with the AS-SIP Specification.

The end instrument is an application running on an XP-embedded platform providing telephony features and Assured Services support on a 5 in. x 4 in. touch screen. Phase 2 will demonstrate a prototype interface to support these features in accordance with the Assured Services SIP Specification.

The device is designed for configurable constraints on resource priorities and precedence domains with support for preemption tones and response codes.

2.1.1 L3_AS_SIP_Phone Installation

The AS-SIP end instrument is installed by:

1. Creating a C:\L3_AS_SIP folder,
2. Copying application and configuration files to the C:\L3_AS_SIP folder,
3. Running the program dotnetfix.exe if Visual Studio is not installed,
4. Updating and saving L3_AS_SIP.xml, as defined in paragraphs 2.1.1.1 and 2.1.1.2.

2.1.1.1 L3_AS_SIP_Phone Configuration

The L3 AS-SIP end instrument is configured by the default editable XML file L3_AS_SIP.xml. The **sip_config_settings** parameters for **proxy_ip** and *username* password need to correspond to the signaling appliance serving proxy and username/password configured on the SIP signaling appliance. Required XML configuration parameters are shown in Table 2-1.

Table 2-1 L3_AS_SIP XML

XML Element	Description
as_sip_proxy	SIP Proxy IP Address
as_sip_local_address	IP Address of AS-SIP Phone
as_sip_local_domain	Local Domain
as_sip_local_authen_username	AS-SIP Phone Username
as_sip_local_authen_password	AS-SIP Phone User Password
as_sip_name_server_ip_address	Name Server IP Address
as_sip_resource_priority_default	Options: routine, priority, immediate, flash, flash-override
as_sip_resource_priority_max	Options: routine, priority, immediate, flash, flash-override (highest allowable priority for end instrument)
as_sip_precedence_domain_default	dsn-000000

2.1.1.2 Configuration Parameters

Figure 2-1 is an example of an operational configuration XML file. Additional configuration parameters can be set which manipulate the button and menu settings further discussed in paragraph 2.1.7.

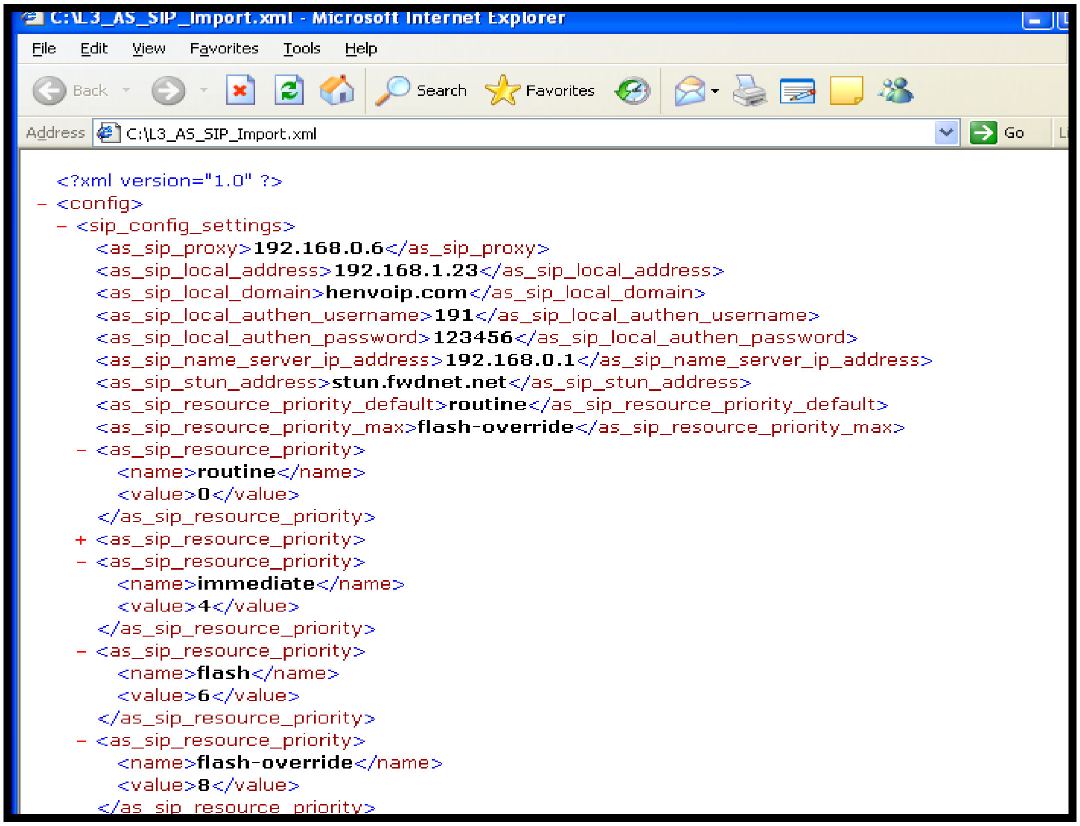


Figure 2-1 L3_AS_SIP XML Configuration File

After updating the configuration file, re-start AS-SIP Phone or load the configuration selecting the **Load Config** button from the CONFIGURATION Menu (see Configuration Mode). Changes can be exported using the **Save Config** button on the CONFIGURATION Menu.

2.1.2 L3_AS_SIP_Phone Usage

2.1.2.1 Starting L3_AS_SIP_Phone

To start L3_AS_SIP_Phone, click on the L3_AS_SIP_Phone.exe file (note that the .exe extension in L3_AS_SIP_Phone.exe may not be displayed).

2.1.2.2 Exiting L3_AS_SIP_Phone

Exit L3_AS_SIP_Phone by clicking the L3 image in the lower center of each menu screen (Figure 2-2).

2.1.2.3 Phone Screens

L3 AS-SIP phone screens can be navigated using the screen function key in the lower left corner of the screen which selects the screen mode (in Figure 2-2, the lower left button is

set to **Preset 1**). Along the bottom of each phone screen is the following set of function keys, or buttons, which include:

1. Mode function button
2. Call function button
3. Priority function button
4. Precedence domain button
5. Four line buttons with corresponding information boxes and microphone toggle button.

The L3 AS-SIP phone screen mode function button spans the following:

1. Five **Preset** modes
2. **Dial Pad** mode
3. **Diagnostics** mode
4. **Configuration** mode.

The call function keys consist of:

1. **Call/Hangup**
2. **Hold/Resume**
3. **Forward en/dis**
4. **Transfer**
5. **Redial**
6. **Messages**.

2.1.2.4 Preset Modes

Preset modes are set in the XML configuration file (Figure 2-1) and display text to users mapped to phone numbers sent to the SIP Proxy.

2.1.2.5 Placing Calls

1. Select call function key (**Call/Hangup** is the default).
2. Select line button (for example, press line button **Line 1,** observe button border is darkened for selected line).
3. Select **Preset** button.

The number associated with that button will be sent to the proxy. Other functions applicable to **Preset** mode screens are detailed in paragraph 2.1.5.

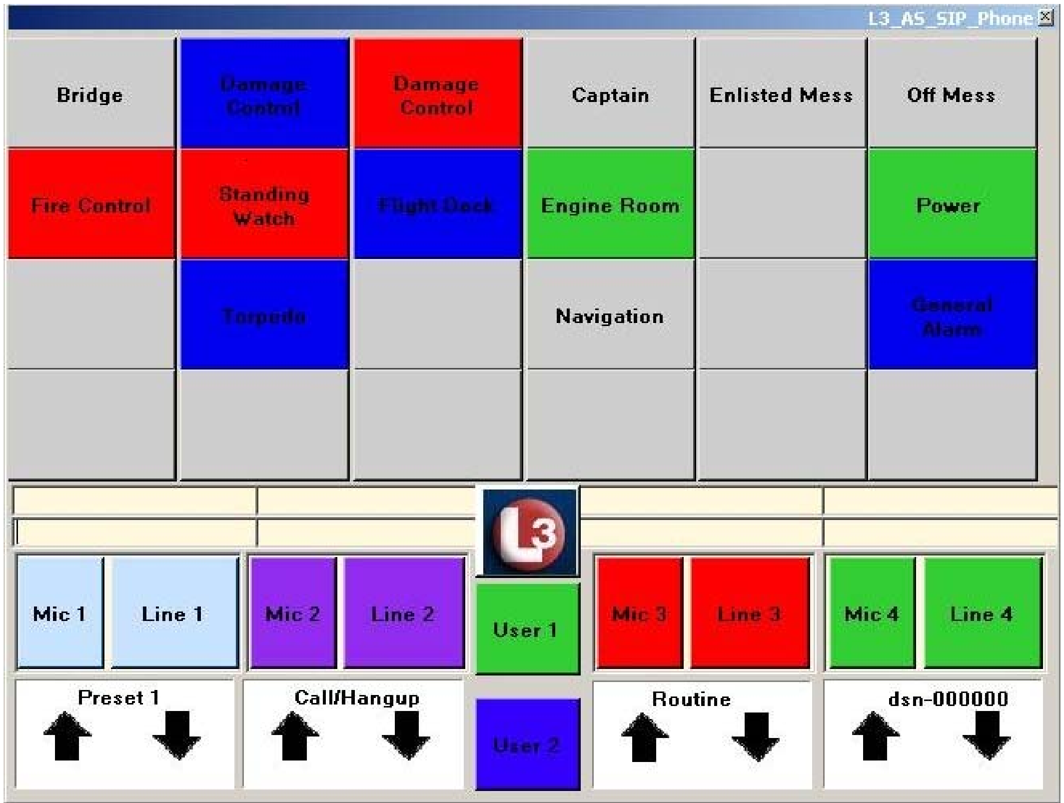


Figure 2-2 L3_AS_SIP_Phone GUI Sample Preset Menu

2.1.2.6 Dial Pad Mode

The Dial Pad Screen is displayed after hitting the **Mode** button until **Dial Pad** is displayed on the **Mode** button.

2.1.2.7 Placing Calls

1. Select function (**Call/Hangup** is the default).
2. Select line (press **Line** button, for example **Line 1)**. Observe button border is darkened for selected line.
3. Press number keypad for number to be called.
4. Observe number in corresponding line information box.
5. Initiate call by pressing **CALL** button (Figure 2-3, second button from right on top line of dial pad).

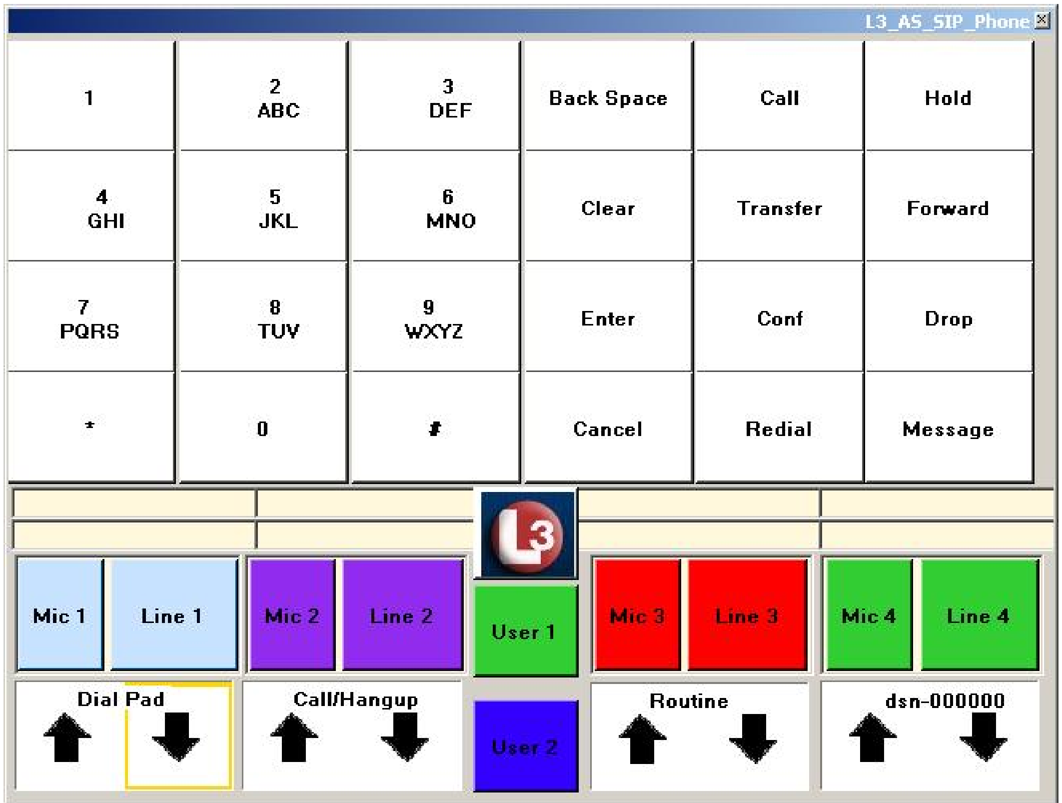


Figure 2-3 L3_AS_SIP_Phone GUI Sample Dial Pad Menu

2.1.3 Configuration

The **Configuration** screen provides a Windows interface to modify or load the configuration maintained in the XML file. Import a configuration using the **Load Configuration** button (Figure 2-4). Configuration data from \L3_AS_SIP.xml is used to configure the end instrument. Export the currently loaded configuration by pressing the **Save Configuration** button. The currently loaded configuration is written to L3_AS_SIP.xml.

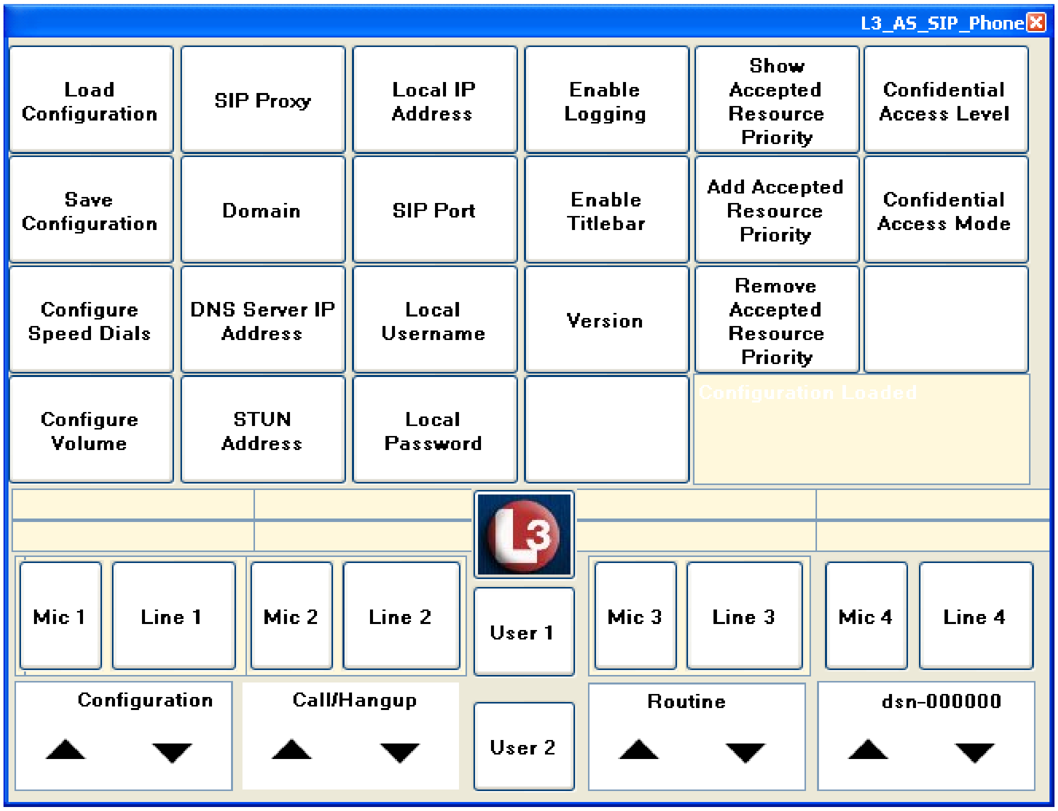


Figure 2-4 L3_AS_SIP_Phone GUI Configuration Menu

2.1.3.1 Configure Speed Dials

The Speed Dial configuration allows the developer to configure the speed dials without having to access the XML configuration file. It is a boolean button so you press it again to leave the mode. In this mode the *On-Screen Keyboard* window is launched so information can be entered without connecting a keyboard. This feature was for development purposes only and is not expected to continue to a production version.

2.1.3.2 Speed Dials Dialogue Box

Figure 2-5 is the dialog box to configure the speed dial and Figure 2-6 is the *On-Screen Keyboard* window. The **Type:** is a defined list that you can select; the type controls the color of the button.

Figure 2-5 Speed Dial Configuration Dialogue Box

Figure 2-6 On-Screen Keyboard Window

2.1.4 Diagnostics

The **Diagnostics** screen (Figure 2-7) provides the developer with a tool to allow for testing and debugging of the unit. Since this screen is for developers its contents have changed several times during the development process. At this time the screen only contains **Start Trace** and **End Trace**, the other functions have been moved to the configuration screen. The trace functionality is done using WinPcap (http://www.winpcap.org) that allows tracing to be done at the network packet level, and viewed in Wireshark (http://www.wireshark.org).

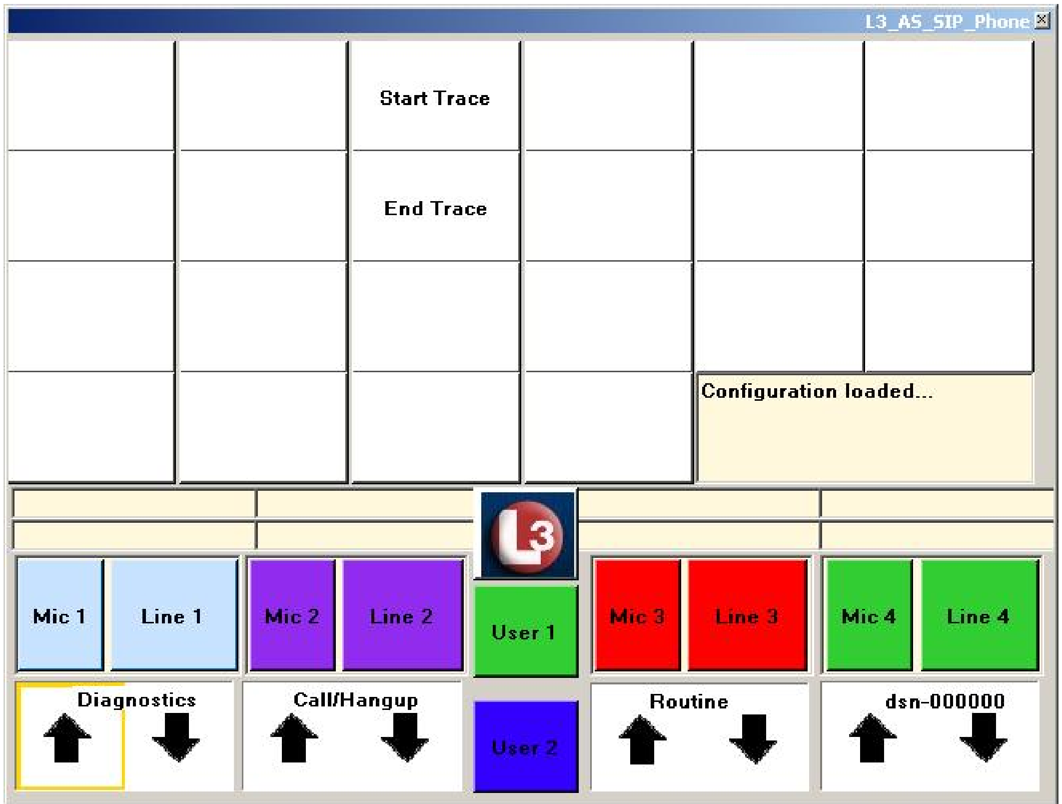


Figure 2-7 Diagnostics Screen

2.1.5 Telephony Functions

2.1.5.1 Answering Calls

The line button on the line corresponding to the inbound call will flash **RING** in red. Press the line button and the incoming call will become active and the line will indicate this by changing the line button green and relabeling the button as **Active**.

2.1.5.2 Call/Hangup

To place calls:

1. Select mode **Call/Hangup.**
2. Select **Line** (observe darkened border).
3. Press **Preset** or **Dial Pad** numbers (see paragraphs 2.1.2.4 and 2.1.2.6).
4. **Dial** will appear in line button with orange background until call is active or terminated.
5. Voice path will be established when called party answers and line button text will read **Active** with a green background.

Note: To cancel call, press line button and the line number text will be displayed in the line button.

To terminate calls:

1. Select mode **Call/Hangup**
2. Select **Line** (observe darkened border).
3. Line button will no longer indicate **Active** and the button text will indicate the line number. Voice path will be torn down.

2.1.5.3 Hold/Resume

To place a call on hold:

1. Select Mode **Hold/Resume**.
1. Select **Line** (observe darkened border).
2. Observe line button, **HOLD** will appear in line button with red background.
3. Voice path is suspended.

To resume a call on hold:

1. Select Mode **Hold/Resume**.
2. Select **Line** (observe darkened border).
3. Voice path will be established when called party answers and line button text will read **Active** with a green background.

2.1.5.4 Forward Enable/Disable

To forward calls:

1. Select Mode **Forward en/dis**
2. Select **Line** (observe darkened border).
3. Line corresponding information text box will instruct User to input forwarding number. If in **Preset** mode, select **Preset** button. If in **Dial Pad** mode, enter number, the press forward.
4. Forwarding message and address is displayed for corresponding line.

To cancel call forwarding:

1. Select mode **Forward en/dis**
2. Select Line (observe darkened border).
3. Voice path will be established when called party answers and line button text will read **Active** with a green background.
4. Line button text will indicate the line number.

2.1.5.5 Transfer

To transfer calls:

1. Select mode **Transfer**.
2. Select **Line** (observe darkened border).

3. Line corresponding information text box will instruct use to input transfer number. If in preset mode, select preset button. If in **Dial Pad** mode, enter number, the press **Forward**.
4. Transfer message and address is displayed for corresponding line.
5. Corresponding line button and information boxes are reset.

2.1.5.6 Redial

To redial number:

1. Select mode **Redial.**
2. Select **Line** (observe darkened border).
3. Line corresponding information text box will indicate the redialed number.
4. **Dial** will appear in line button with orange background until call is **Active** or terminated.
5. Voice path will be established when called party answers and line button text will read **Active** with a green background.

2.1.6 Resource Priority

Outgoing calls will include a resource priority header with value (Table 2-2). The resource priority button can be pressed and the priorities are displayed sequentially in priority order. When the call is initiated, the priority indicated by this button will be placed in the resource priority header as seen in Figure 2-8.

Table 2-2 Resource Priority Decimal Values

r-priority	CORRESPONDING DECIMAL VALUE
routine	0
priority	2
immediate	4
flash	6
flash-override	8

2.1.6.1 Precedence Domain

Outgoing calls will include precedence domain in the resource priority header. The precedence domain button can be pressed and the precedence domains are displayed sequentially. The default is dsn-000000. When the call is initiated, the precedence domain indicated by this button will be placed in the resource priority header as seen in Figure 2-8.

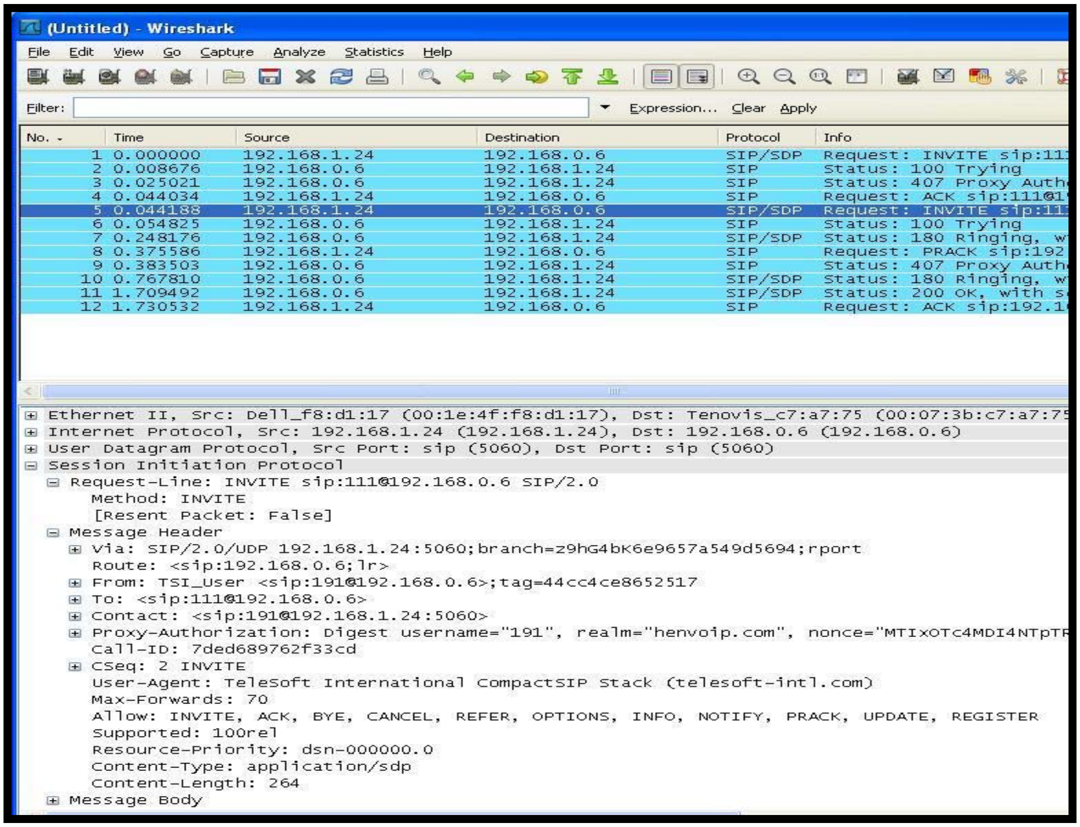


Figure 2-8 L3 AS-SIP Phone Resource Priority Protocol Trace

In the above protocol trace, the SIP Message Header contains a "Resource Priority" header of dsn-000000.0. This corresponds to the default precedence domain (dsn-000000) and routine priority call (.0).

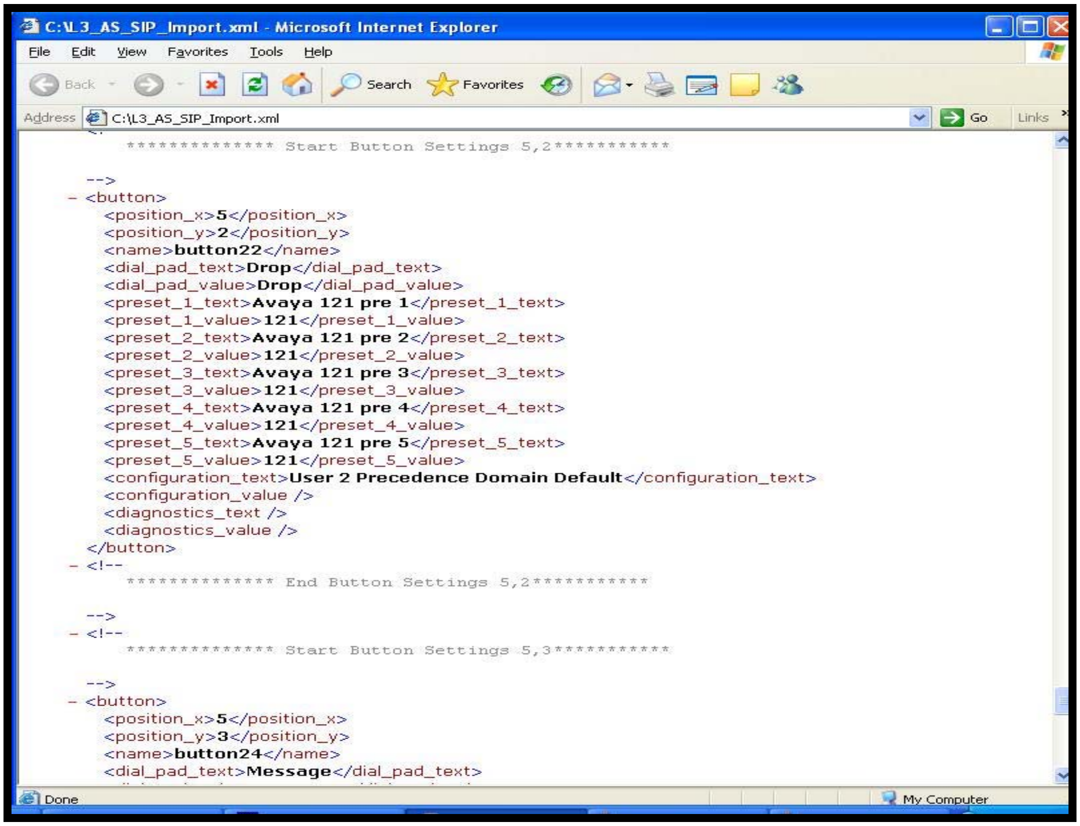
2.1.6.2 L3_AS_SIP_Phone Interoperability Tests

Appendix B describes interoperability tests to be performed using call functions described in paragraph 2.1.5.2. Because the UCR does not at this time define the requirements for end devices working with AS-SIP, tests were used to check the compatibility between devices. The testing was done between PoCs as well as with REDCOM.

2.1.7 Button and Menu Settings

2.1.7.1 Button Settings

Button settings are defined in L3_AS_SIP.xml (Figure 2-9). The settings define what is displayed to the user on end instrument buttons, and the values which are sent by the application to the SIP signaling appliance.

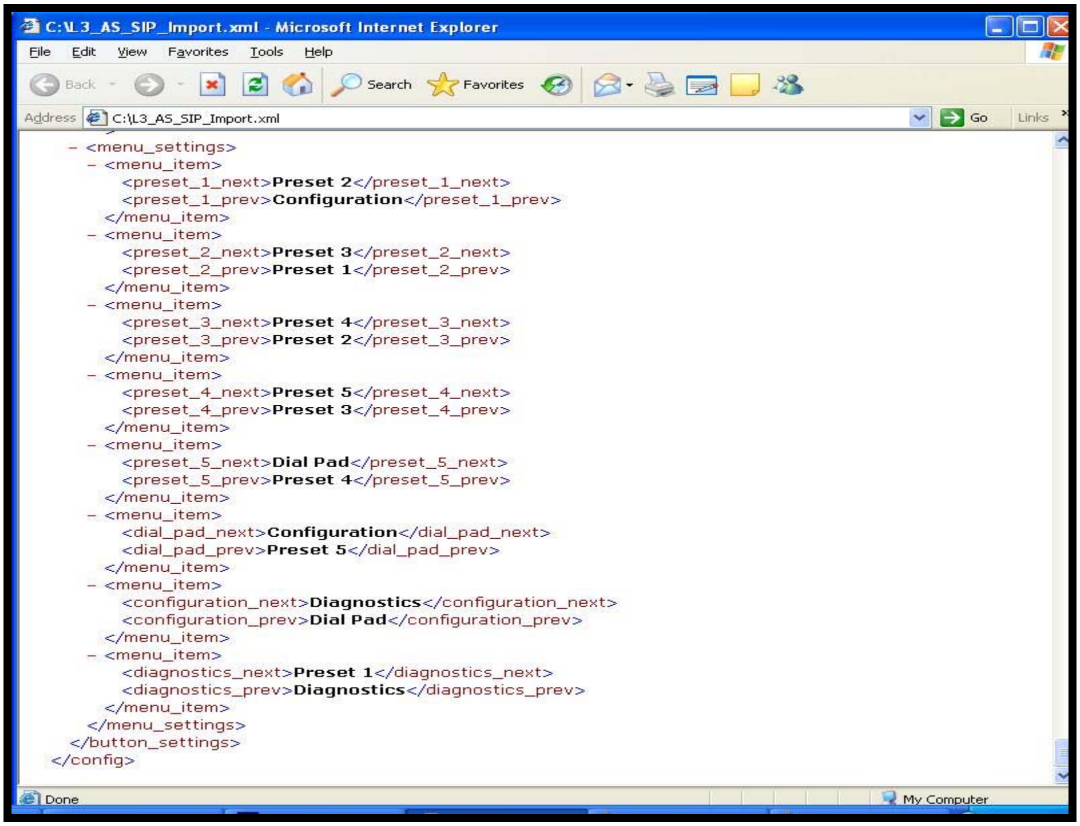


```
C:\L3_AS_SIP_Import.xml - Microsoft Internet Explorer
      *************** Start Button Settings 5,2***********
  -->
- <button>
    <position_x>5</position_x>
    <position_y>2</position_y>
    <name>button22</name>
    <dial_pad_text>Drop</dial_pad_text>
    <dial_pad_value>Drop</dial_pad_value>
    <preset_1_text>Avaya 121 pre 1</preset_1_text>
    <preset_1_value>121</preset_1_value>
    <preset_2_text>Avaya 121 pre 2</preset_2_text>
    <preset_2_value>121</preset_2_value>
    <preset_3_text>Avaya 121 pre 3</preset_3_text>
    <preset_3_value>121</preset_3_value>
    <preset_4_text>Avaya 121 pre 4</preset_4_text>
    <preset_4_value>121</preset_4_value>
    <preset_5_text>Avaya 121 pre 5</preset_5_text>
    <preset_5_value>121</preset_5_value>
    <configuration_text>User 2 Precedence Domain Default</configuration_text>
    <configuration_value />
    <diagnostics_text />
    <diagnostics_value />
  </button>
- <!--
      *************** End Button Settings 5,2***********
  -->
- <!--
      *************** Start Button Settings 5,3***********
  -->
- <button>
    <position_x>5</position_x>
    <position_y>3</position_y>
    <name>button24</name>
    <dial_pad_text>Message</dial_pad_text>
```

Figure 2-9 L3 AS-SIP Phone Button Configuration XML

2.1.7.2 Menu Settings

Menu are managed via a linked list defined L3_AS_SIP.xml (Figure 2-10). The settings define Mode display attributes. Using next and previous tags, menu order can be manipulated and menus removed.




```
- <menu_settings>
  - <menu_item>
      <preset_1_next>Preset 2</preset_1_next>
      <preset_1_prev>Configuration</preset_1_prev>
    </menu_item>
  - <menu_item>
      <preset_2_next>Preset 3</preset_2_next>
      <preset_2_prev>Preset 1</preset_2_prev>
    </menu_item>
  - <menu_item>
      <preset_3_next>Preset 4</preset_3_next>
      <preset_3_prev>Preset 2</preset_3_prev>
    </menu_item>
  - <menu_item>
      <preset_4_next>Preset 5</preset_4_next>
      <preset_4_prev>Preset 3</preset_4_prev>
    </menu_item>
  - <menu_item>
      <preset_5_next>Dial Pad</preset_5_next>
      <preset_5_prev>Preset 4</preset_5_prev>
    </menu_item>
  - <menu_item>
      <dial_pad_next>Configuration</dial_pad_next>
      <dial_pad_prev>Preset 5</dial_pad_prev>
    </menu_item>
  - <menu_item>
      <configuration_next>Diagnostics</configuration_next>
      <configuration_prev>Dial Pad</configuration_prev>
    </menu_item>
  - <menu_item>
      <diagnostics_next>Preset 1</diagnostics_next>
      <diagnostics_prev>Diagnostics</diagnostics_prev>
    </menu_item>
  </menu_settings>
 </button_settings>
</config>
```

Figure 2-10 L3 AS-SIP Menus Configuration XML

2.1.8 Conclusion

The Proof-of-Concept is the first Assured Service-SIP device to be created (to L-3 Henschel's knowledge). It proves that protocol will work for an end device, and allow for unified network applications to be enabled on a naval vessel. Even though the UCR did not embrace end devices in its first release, it will in future releases. This document delineates in great detail the hardware and software research and development that went into the Proof-of-Concept device, from a user's perspective.

2.2 Hardware Development

2.2.1 Hardware Selection

The Proof-of-Concept (PoC) is to test the Assured Services SIP (AS-SIP) protocol in a lab environment. This will allow sailors to see how it performs in the current CIVUT environment (or any other vendors terminal), thereby reducing the learning curve and allowing them to use their current knowledge. The design is reduced in height from the current unit but its footprint is the same, so it could be used on a vessel in the same location as the current unit. The vessel for Trident Warrior 2009 was not known at the beginning of the project so maintaining the footprint was a benefit. In the end, the project changed as Avaya was not able to support AS-SIP end devices on Trident Warrior so the maintaining of the footprint had less value, but the overall layout was completed and the material developed.

2.2.1.1 Processor

The processor card needed to include as many of the Input/Output (I/O) as possible but still maintain a compact size. To reduce complexity of the project it was decided to us e PC/104 form facture. Since the project is to show the feasibility of VoIP, this form facture allowed for a smaller final device. The module needed to contain at a minimum network, sound, USBs, video, and the hard drive controller. To support the SIP stack (which was not defined) we needed to have the processor power and memory to support the application under review; the decision was made to look at a Pentium M processor. This had issues of heat dissipation that would need to be dealt with during the design phase.

The MPL-10 card from MPL was selected because it had the processor as well as I/O required for the initial proof-of-concept design. The first major issue was heat dissipation. This was resolved by placing the CPU against an aluminum plate that would be in contact with a surface that would draw the heat away from the module. During initial testing it was found to work well with the unit placed onto a piece of aluminum and allowed to run for extended length of time. The MPL-10 is equipped with I/O that covered many of the requirements, but not all of them. It only had a single network interface and AC97 sound bus. It did contain four USB interfaces, DVI-I video and a Serial ATA bus to connect a drive. This was adequate for the initial design of the PoC. The MPL-10 processor also has an aluminum mounting plate for heat dissipation (Figure 2-11). The connectors on the board are all Molex Pico locking clips. It is a two-board stack with the processor on the bottom board and the top board handling the input\output functionality.

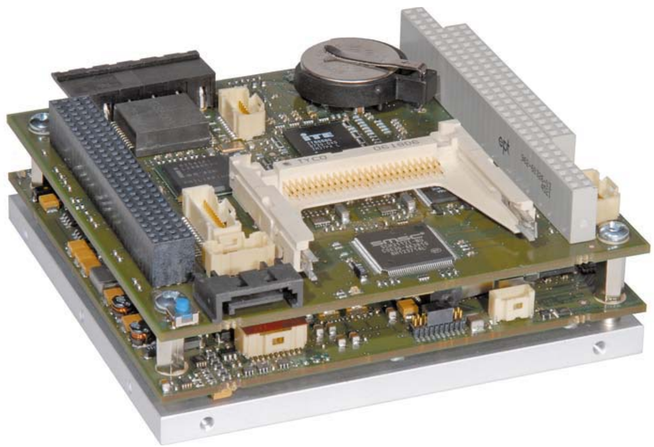


Figure 2-11 MPL-10

2.2.1.2 Hard Drive

The initial direction was to use a Compact Flash (CF) to contain the operating system and application. This technology is currently used for the DOS application and has shown stability over the years. However, during research several issues arose when testing the CF for Windows XP embedded (XPe). The initial problem stems from a couple of different areas: most CF are made for the consumer market place and are setup as a removable devices. This limits the functionality when used as a hard drive. The operating system will not allow configuration with a boot sector. This can be resolved by pushing an image that includes the boot sector onto the CF, and adding the XPe image developed with the Microsoft Windows Embedded Development Environment. The First Boot Agent will then setup the drive for the operating system. However this creates a problem with the performance of the system; the OS will not allow setup of a swap file. The solution is to convert the CF to a fixed drive. Many vendors do not support this and do not have a tool to convert the drive from “removable” to “fixed”. SanDisk provided an executable to convert the CF to fixed but let it be known that it would void the warranty of the CF and the hard drive. They have a line of CF for commercial applications, but they do not recommend its use for the hard drive for XPe. Coremicro has a CF product line that can be used for this application and would support the implementation of XPe. After more research it was found that the CF has a limited number of read-write cycles and the OS background processes will vastly shorten the life of the CF card. There are registry changes that can be made to the OS to reduce the number of writes, but even with that ability several of the manufacturers did not recommend the use of their products for use as a hard drive for XPe.

The use of a solid-state drive (SSD) (Figure 2-12) fulfills the requirements for shock and vibration. Several of the different manufactures manufacture many different sizes of SSD. The other benefit is a larger SSD than CF for only a slightly higher price. In this case the drive will be a SATA drive that connects to the MPL-10. In the BOIS it must be set for “S-ATA Only” mode. The MPL-10 only supports CF or a drive connected to the SATA port. If connected to a standard hard drive port, the BOIS can be set to “P-ATA Primary”, but a SSD drive has to have the BOIS set to “S-ATA Only” for it to be recognized. Refer to paragraph 2.2.3 for more details on the performance differences between the three types.

.

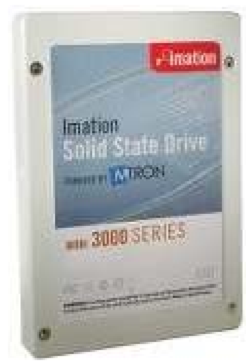


Figure 2-12 Imation Solid State Drive

2.2.1.3 Sound Cards

The MPL-10 has a single AC97 chipset for the sound solution. This allows for one stereo speaker output and microphone, but multiple user systems need to have multiple sound cards. If there is a requirement for a speaker phone function, then a separate sound card will be required. Multiplexing can also be evaluated but no COTS product was found that allowed for multiple microphone input. It may be cost effective to have a custom designed sound card that takes in multiple microphone inputs and allows selection of them in single or multiple groupings. It would also be useful to be able to mix the different inputs into a single stream so that two users can conference together at the sound card level; but this type of conferencing can also be done in SIP.

It was chosen to implement with the MPL-10 sound card for User 1 and two USB sound cards for User 2 and the speaker phone. The decision was driven by the cost and size of adding PC/104 sound cards and increasing the stack height of the MPL-10 by 1 inch. In the original PoC design a single user was going to be supported, but in discussions it was felt that multiple user support was needed, but it was left off because of timing. It was determined that technically it was not a problem to be added at a future time.

2.2.1.4 Power Supply

The initial power supply was a standard cased unit that was larger then the MPL-10 unit. In review with L-3 Henschel Electrical Engineering they had a very small unit that could be contained within the PoC. Working with Trident Warrior 2009 group and the lack of information about the LHA4 Nassau's power requirements; it was determined that we would use an external AC-DC converter. This would allow the PoC to be connected to 110V AC if required by the location of the units for the test. The internal power supply has a large range of DC voltages to allow it to work in a large band of different voltages. Because of the current head design the possibility of Power over Ethernet (PoE) is not possible with the current display. This can be remedied with the right selection of display.

2.2.1.5 Display Head

The display head that was used is from L-3 Henschel's current product line (Figure 2-13). Since the task was for feasibility of VoIP, development of a new head was not necessary to fulfill the required tasks. For a future design, the head should be changed for several reasons. The head currently is VGA with a resolution is only 640 X 480; but the MPL-10 supports DVI-I. An increase in resolution would be supported by Windows XP directly, without warnings for low resolution. The refresh rate could be increased from the current 60 hertz. The head is designed around serial communications, and USB could be changed to have a USB hub internal to the unit which only requires a single connection to the head and has the sound card incorporated into the head design. The MPL-10, like several other modules, also has other features that can be off-loaded from the head to the module to reduce overall complexity of the head, assisting in the ability for separation between call channels. The head unit will stay a custom part, but should be able to contain more functionality in a smaller overall size.

Figure 2-13 Proof-of-Concept

2.2.2 Packaging of Hardware

2.2.2.1 Processor Heat Dissipation

One of the issues to work through for this project was heat dissipation from the processor that was specified in the design. In future designs the processor may be reduced, but to hold down the cost of the design a Pentium M was chosen so no special development tools were required and the development could be done on standard desktop PCs.
The processor is thermally coupled to an aluminum plate at the bottom of the MPL-10 stack. This dissipates the heat from the processor to the plate. The plate is then coupled with heat transfer material to the external case, allowing the heat to be dissipated from the internal of the PoC to the external case. This solution has worked for the PoC, but should be evaluated for the solution as it moves forward. Final testing determined that a small fan was required to dissipate the heat build-up in the enclosed PoC. The fan exhausts from the bottom of the unit; a fan to circulate the air may have been all that was required.

2.2.2.2 Reduced Size

Size, even though not part of the feasibility study, was an issue as the concern was to at least maintain the current footprint. The stack of PC/104 cards was reduced from the current BRI product by removing the proprietary BRI and audio cards. The audio card

was replaced with the one contained in the MPL-10 and two USB units for the second user and the speaker phone. With that reduction, we were able to reduce the height of the unit while the footprint size was maintained. For ease of use the PoC was attached to a piece of aluminum with the handset cradles connected to it. In future PoCs, the MPL-10 could be replaced with a single module card and integrated into the display head. The footprint cannot be reduced by any major amount because of the size of the current display. Better graphical user interface design may allow for small reductions in space, but if the unit is used with the touch screen with a finger as the stylus, the overall screen size can not be reduced and still maintain the number of required buttons (Figure 2-14).

Figure 2-14 Completed Proof-of-Concept

2.2.3 Performance Benchmarks

The different types of hard drives were benchmarked to evaluate their performance and their effect on the other major components of the MPL-10. The three types tested were compact flash, solid state drive, and a standard mechanical hard drive. Each type has its benefits and drawbacks. The preference was the compact flash - it is very compact and its socket is on the MPL-10 so no other space was required. It has no mechanical parts so vibration and shock are not an issue. The solid state drive also has no mechanical parts, but does require mounting space for the unit and wires. The hard drive has both problems - it is a mechanical device and requires space to locate it in the PoC. The

benchmarking was done with the Generated by FreshDiagnose (c) 2008, FreshDevices Corp., tool that worked well for this limited test. It will not do a compact flash card that is a removable media, but will if it is set as fixed media.

The first test was to determine the performance of the different types of hard drives (Figure 2-15). As noted the write speed of the solid state devices is much slower than the hard drive. The solid state drive has the fastest read times of the three devices. In this case the PoC will be doing limited writing in normal operations, so the solid state drive appears to be the best choice.

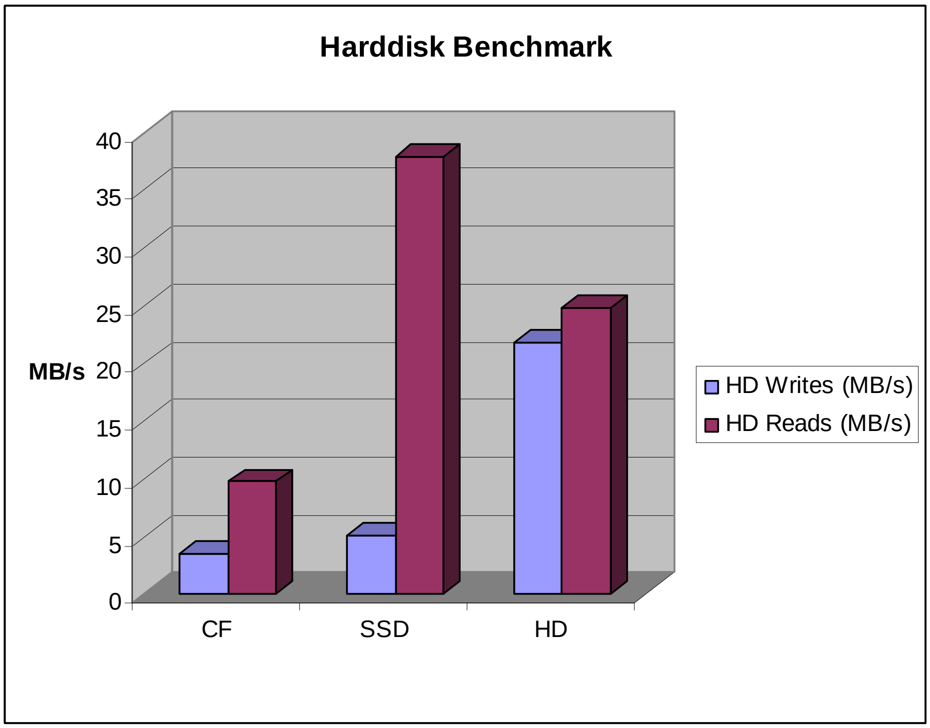


Figure 2-15 Hard Disk Benchmark

The rest of the tests were to see if the drive type reflected on the performance of other major components of the MPL-10; as shown there was little difference between the three types of drives (Figure 2-16 thru Figure 2-18, and Table 2-3).

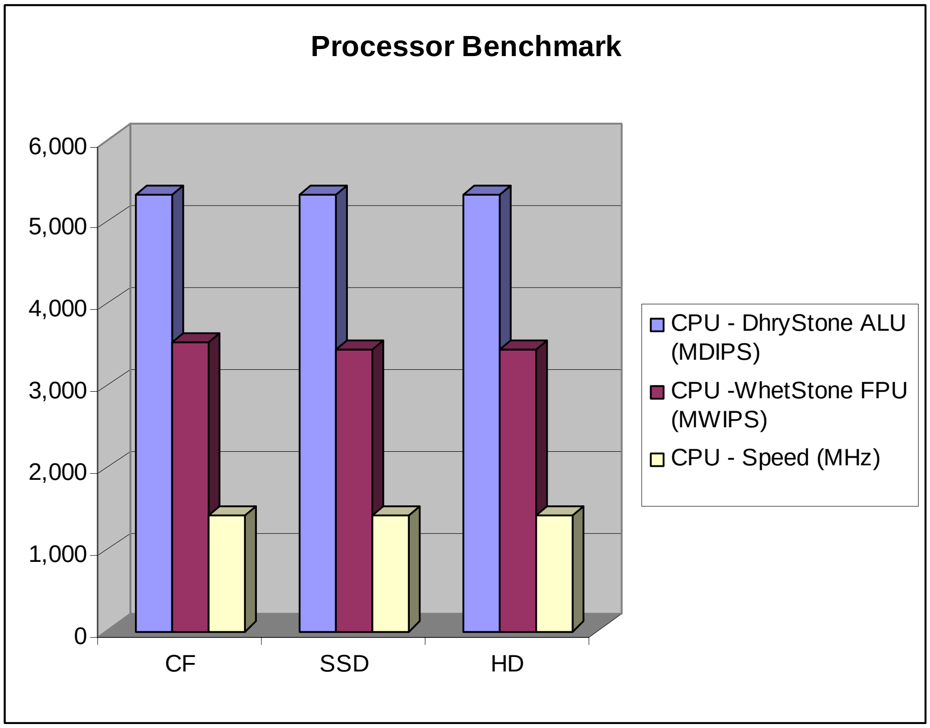


Figure 2-16 Processor Benchmark

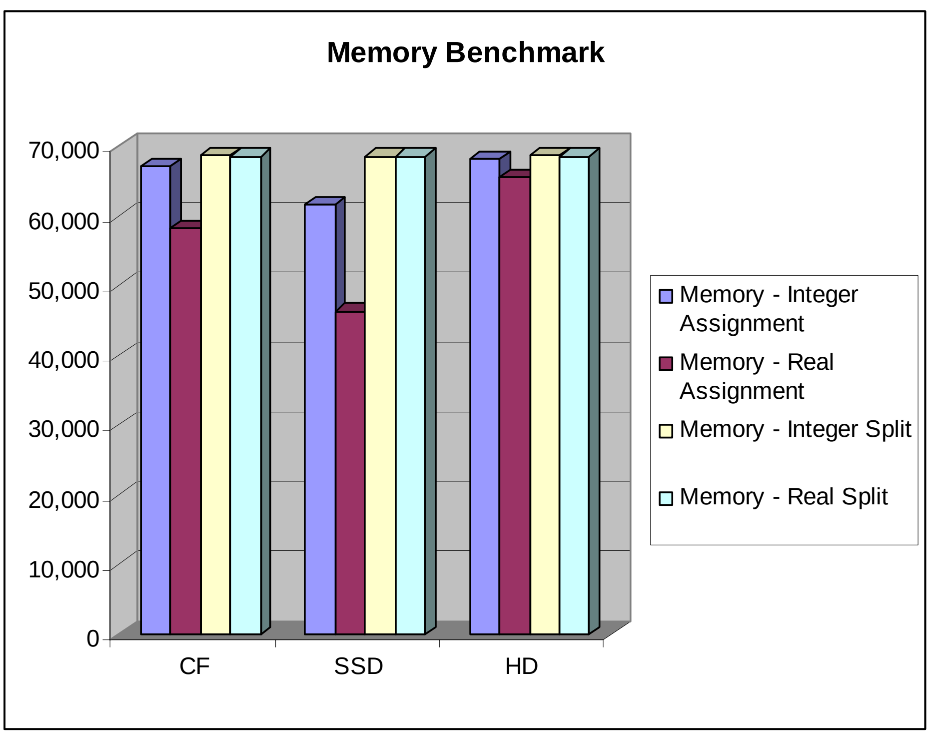


Figure 2-17 Memory Benchmark

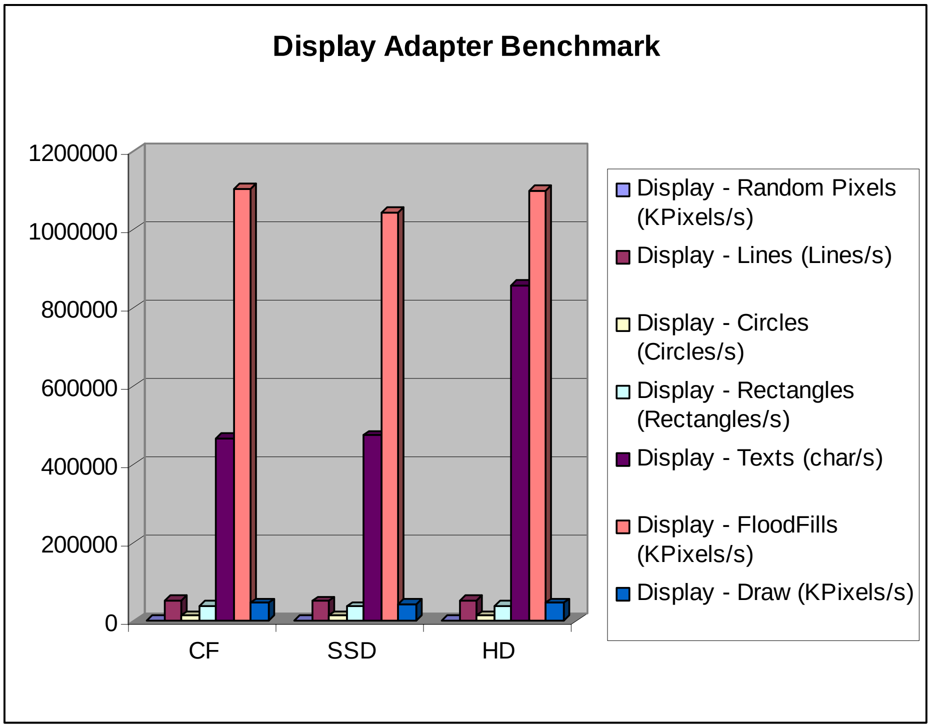


Figure 2-18 Display Adapter Benchmark

Table 2-3 Hard Drive Raw Test Data

	CF	SSD	HD
HD Writes (MB/s)	3.48	5.05	21.86
HD Reads (MB/s)	9.74	37.89	24.81
Memory - Integer Assignment	67,070	61,524	68,108
Memory - Real Assignment	58,295	46,335	65,568
Memory - Integer Split	68,576	68,536	68,667
Memory - Real Split	68,523	68,509	68,515
CPU - DhryStone ALU (MDIPS)	5,327	5,325	5,331
CPU -WhetStone FPU (MWIPS)	3,524	3,432	3,435
CPU - Speed (MHz)	1,402	1402	1402
Display - Random Pixels (KPixels/s)	433	433	433

Table 2-3 Hard Drive Raw Test Data - Continued

	CF	SSD	HD
Display - Lines (Lines/s)	52,333	50,666	52,000
Display - Circles (Circles/s)	13,125	13,005	12,958
Display - Rectangles (Rectangles/s)	37,715	36,768	38,266
Display - Texts (char/s)	467,030	475,151	858,494
Display - FloodFills (KPixels/s)	1,106,720	1,044,160	1,100,320
Display - Draw (KPixels/s)	44,441	42,803	44,304

2.2.4 Conclusion

Because of the operational performance of the Compact Flash and the manufacturers not promoting it for use as hard drives for Windows XP, we decided to use a solid state hard drive. The write speed of the compact flash is slower then the hard drive, but the survivability of the hard drive using COTS products is a problem. The conclusion is the solid state drive will be used for the PoC.

CHAPTER 3 iACT AS-SIP IP COMMUNICATIONS TERMINAL RESEARCH

3.1 Introduction

This section contains a summary of research and implementation findings for iACT Phase 2 Assured Services SIP Proof-of-Concept (PoC) software development, including the following:

- A description of the PoC software architecture, design and implementation details,
- A description of the PoC software development environment, build environment, and installation,
- A description of the PoC software security,
- A description of development platform options and decisions,
- A description of the functional usage of the PoC, and
- Overview of Assured Services SIP (AS-SIP) from an end device perspective.

This section provides a description of the different files and objects within the code. This will allow the user to use the current code base and purchase Telesoft and Global IP Solutions (GIPS) licenses to build the product and understand its functionality. The code is contained on the DVD that is included with this document.

The code is limited to L3 Henschel AS-SIP development for iACT Phase 2 AS-SIP. During this phase, modifications were also made to the Telesoft SIP stack supporting resource priority, accepted resource priority, and confidential access level headers. A license for the Telesoft SIP stack and GIPS 3.0 voice engine must be purchased. Support for added headers as modified in the licensed stack is also addressed in this section.

The executable code is written in the C# language and built using Microsoft Visual Studio 2008. The dlls are written in ANSI C/C++.

3.1.1 Proof-of-Concept: Architecture, Design and Implementation Details

The following files are described in this paragraph:

- L3_AS_SIP_Phone.cs
- ASIP_GUI.cs
- ASIP_GUI.Designer.cs
- ASIP_PcapSettingsConfig.cs
- ASIP_PcapSettingsConfig.Designer.cs
- ASIP_SipSettingsConfig.cs

- ASIP_SipSettingsConfig.Designer.cs
- ASIP_SpeedDialConfig.cs
- ASIP_SpeedDialConfig.Designer.cs
- ASIP_SplashScreen.cs
- ASIP_SplashScreen.Designer.cs
- ASIP_CpSIP.cs

3.1.1.1 L3_AS_SIP_Phone.cs

This file contains the code which starts the application.

3.1.1.2 ASIP_GUI.cs

This is the main file for the user interface side of the application defining most functionality, as well as:

- Initiating the system
- Providing the data/function selection mechanism
- Calling into the SIP stack for session control
- Defining callback routine for receiving signals/data from the SIP stack.
- Defining event handlers
- Defining timers.

3.1.1.3 ASIP_GUIDesigner.cs

This file contains code which initializes components and instantiates objects for the GUI, as well as:

- Public static objects are defined in this file
- Default parameter values for object size, location, and text are set for primary menu
- Event handlers are mapped to public static objects.

3.1.1.4 ASIP_PcapSettingsConfig.cs

This file contains the code which defines methods for the **pcap** class used for protocol traces. It also performs the following:

- Initializes Protocol Capture Component
- Defines form for selecting device on which to capture

3.1.1.5 ASIP_PcapSettingsConfig.Designer.cs

This file contains code which instantiates objects and defines properties for the protocol tracing class, as well as:

- Default parameter values for object size, location, and text are set for protocol capture device selection menu
- Event handlers are mapped to public static objects for protocol capture component.

3.1.1.6 ASIP_SipSettingsConfig.cs

This file contains methods for modifying SIP configuration settings defined in the **SipSettingsConfig** class. It also performs the following:

- Defines methods for loading and saving configuration parameters
- Defines event handlers for configuration buttons.

3.1.1.7 ASIP_SipSettingsConfig.Designer.cs

This file contains code which instantiates objects and defines properties for the **SipSettingsConfig** class. It also performs the following:

- Defines class objects for configuration settings.

3.1.1.8 ASIP_SpeedDialConfig.cs

This file contains methods for modifying speed dial configuration settings defined in the **ASIP_SpeedDialConfig** class, and

- Defines methods for configuring speed dial buttons
- Defines event handlers for speed dial buttons.

3.1.1.9 ASIP_SpeedDialConfig.Designer.cs

This file contains code which instantiates objects and defines properties for the **ASIP_SpeedDialConfig** class, and

- Defines class objects for speed dial settings

3.1.1.10 ASIP_SplashScreen.cs

This file contains methods for updating the splash screen used during system initialization.

- Defines delegates and methods for Splash Screen displayed at system startup.
- Defines methods for managing the startup progress bar.

3.1.1.11 ASIP_SplashScreen.Designer.cs

This file contains code which instantiates objects and defines properties for the **ASIP_SplashScreen** class.

- Defines public static object for **SplashScreen** class.

3.1.1.12 L3_AS_SIP_Phone – Code

3.1.1.12.1 Init – Splash Screen

The splash screen is invoked at system initialization and displays the splash screen as the application loads. When the application is fully loaded, the splash screen is disabled (Figure 3-1).

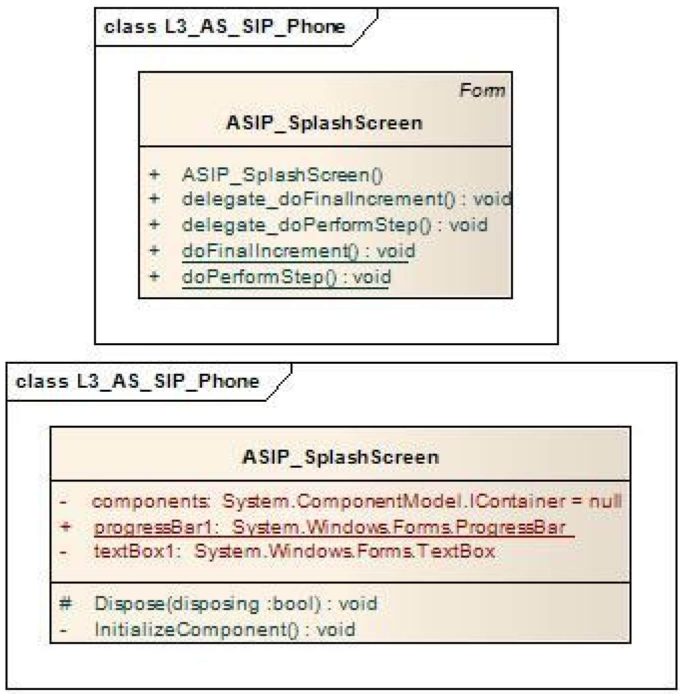


Figure 3-1 Init - Splash Screen

3.1.1.12.2 SIP Setting

The **SIPSettingsConfig** class provides the methods for SIP settings configuration input stored in the **sipCfgParams** data structure (Figure 3-2).

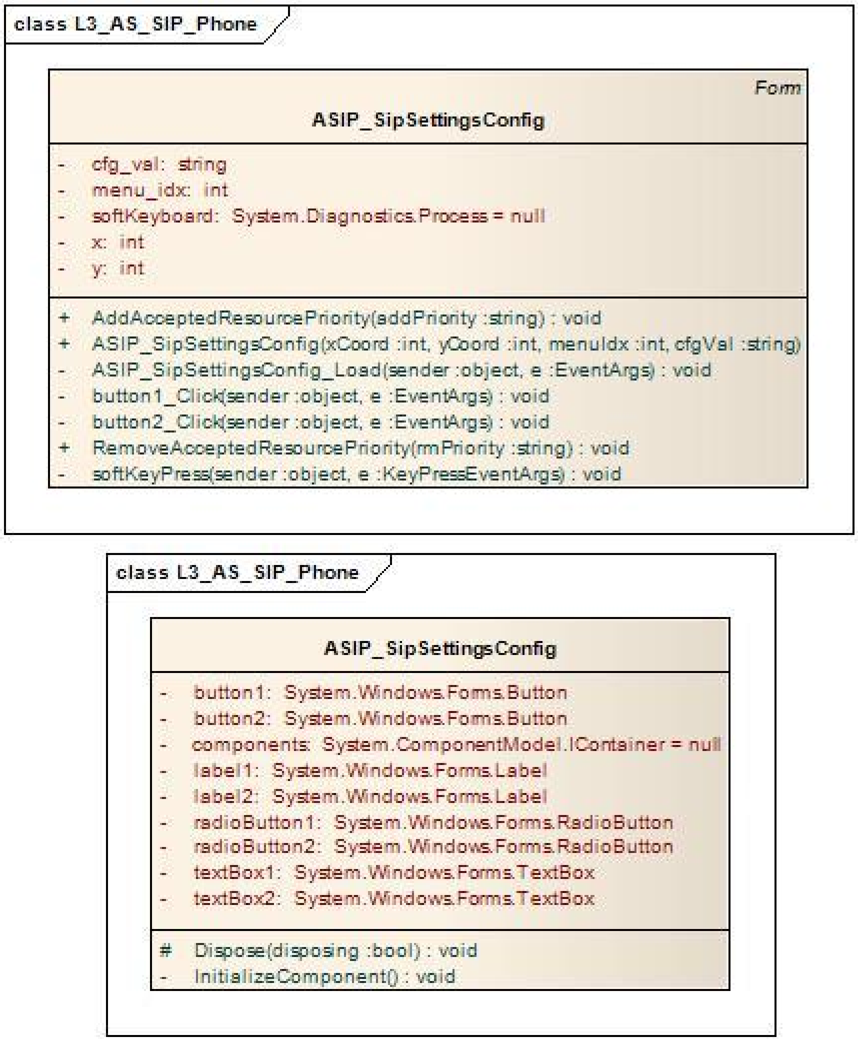


Figure 3-2 SIP Settings

3.1.1.12.3 SpeedDialConfig

The **SpeedDialConfig** class provides the methods for setting the speed dial configuration stored in the **buttondat** data structure (Figure 3-3).

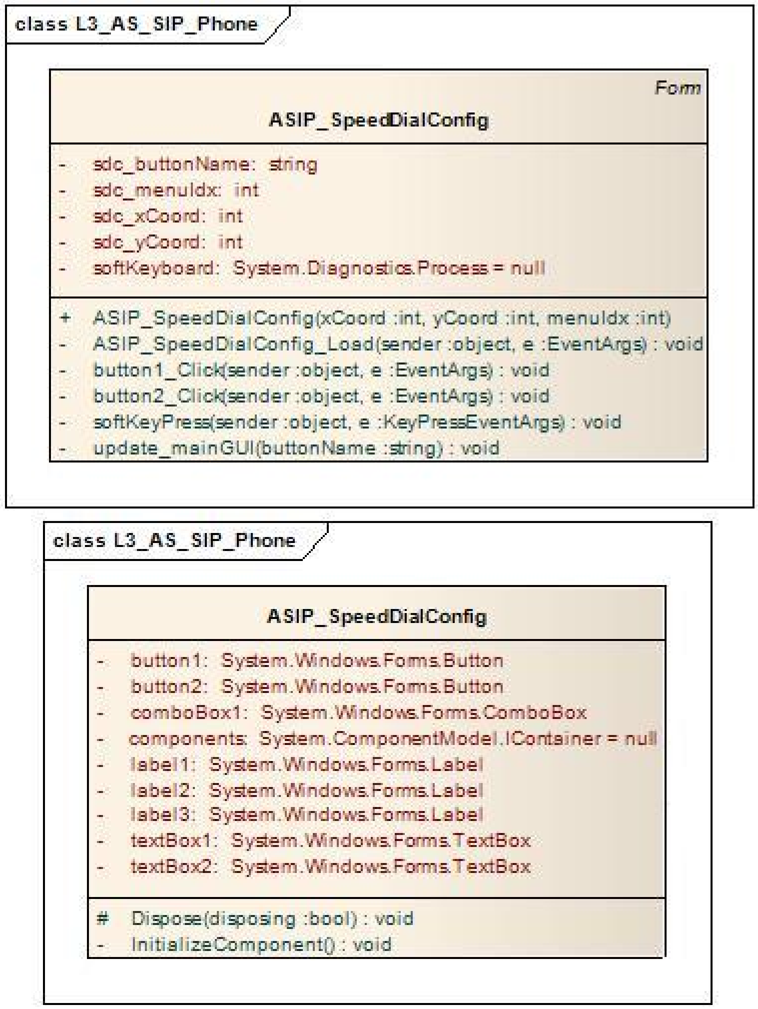


Figure 3-3 Setting Speed Dial Configuration

3.1.1.12.4 Pcap Settings

The **PcapSettingsConfig** class provides the methods for enabling and disabling the SIP protocol tracing (Figure 3-4). This is an open source project that adds link-layer network access in the Windows environment. It allows applications to capture network traffic and store it in a file for later analysis.

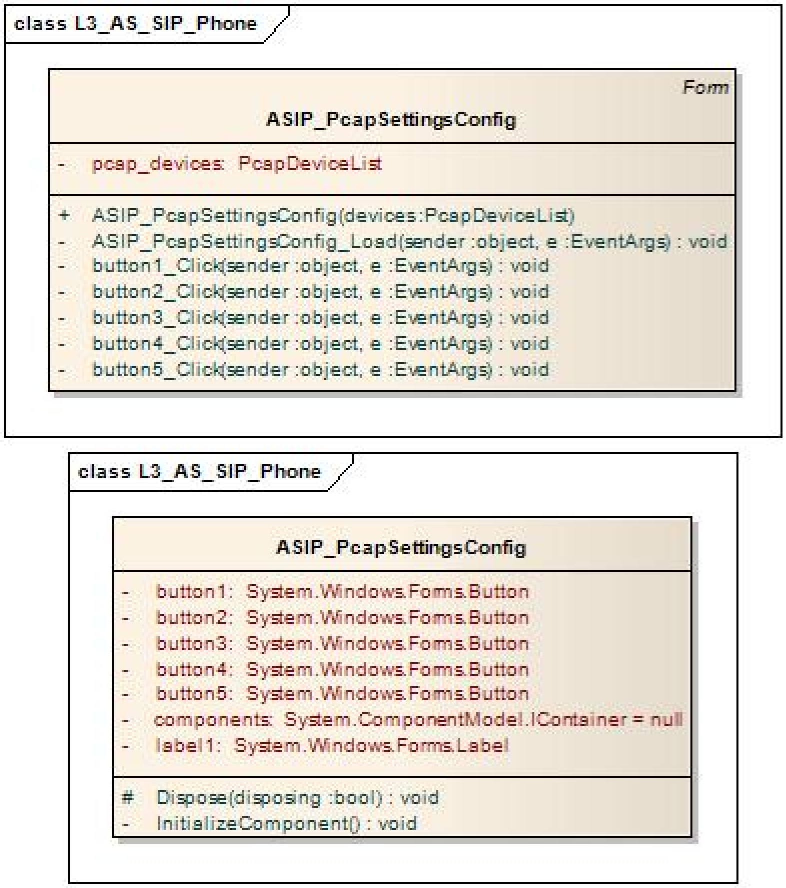


Figure 3-4 Pcap Settings

3.1.1.12.5 ASIP_GUI

The **ASIP_GUI** class provides the methods for initializing and calling methods for user interface control. It includes the definition for input button and output text box objects. It also defines the event handlers and timers (Figure 3-5).

Figure 3-5 ASIP_GUI (Sheet 1 of 7)

```
-  answerbutton_Click(object, EventArgs) : void
+  ASIP_GUI()
-  ASIP_GUI_Closing(object, EventArgs) : void
-  ASIP_GUI_Load(object, EventArgs) : void
+  ASIP_GUICallback(int, int, int, dialog_data*) : void
-  button_Click(object, EventArgs, int, int) : void
-  button1_Click(object, EventArgs) : void
-  button10_Click(object, EventArgs) : void
-  button11_Click(object, EventArgs) : void
-  button12_Click(object, EventArgs) : void
-  button13_Click(object, EventArgs) : void
-  button14_Click(object, EventArgs) : void
-  button15_Click(object, EventArgs) : void
-  button16_Click(object, EventArgs) : void
-  button17_Click(object, EventArgs) : void
-  button18_Click(object, EventArgs) : void
-  button19_Click(object, EventArgs) : void
-  button2_Click(object, EventArgs) : void
-  button20_Click(object, EventArgs) : void
-  button21_Click(object, EventArgs) : void
-  button22_Click(object, EventArgs) : void
-  button23_Click(object, EventArgs) : void
-  button24_Click(object, EventArgs) : void
-  button3_Click(object, EventArgs) : void
-  button4_Click(object, EventArgs) : void
-  button5_Click(object, EventArgs) : void
-  button6_Click(object, EventArgs) : void
-  button7_Click(object, EventArgs) : void
-  button8_Click(object, EventArgs) : void
-  button9_Click(object, EventArgs) : void
-  callbutton_Click(object, EventArgs) : void
-  changeMode_Click(object, EventArgs) : void
-  changeMode2_Click(object, EventArgs) : void
+  clearInfoBox(int) : void
-  configbutton_Click(object, EventArgs, int, int) : void
-  device_PcapOnPacketArrival(object, Packet) : void
-  diagnosticsButton_Click(object, EventArgs, int, int) : void
-  dialpadbutton_Click(object, EventArgs, int, int) : void
-  endTrace() : void
```

Figure 3-5 ASIP_GUI (Sheet 2 of 7)

```
-  exitbutton_Click(object, EventArgs) : void
-  exportButtonConfig() : void
-  forwardbutton_Click(object, EventArgs) : void
-  functionbutton_Click(object, EventArgs) : void
-  functionbutton2_Click(object, EventArgs) : void
-  functionReset() : void
+  getButtonColor(string) : Color
+  getTextColor(string) : Color
-  hangupbutton_Click(object, EventArgs) : void
-  holdbutton_Click(object, EventArgs) : void
-  importButtonConfig() : void
-  launchPcap() : void
-  line1button_Click(object, EventArgs) : void
-  line1mic_Click(object, EventArgs) : void
-  line2button_Click(object, EventArgs) : void
-  line2mic_Click(object, EventArgs) : void
-  line3button_Click(object, EventArgs) : void
-  line3mic_Click(object, EventArgs) : void
-  line4button_Click(object, EventArgs) : void
-  line4mic_Click(object, EventArgs) : void
-  linebutton_Click(object, EventArgs) : void
+  lineInfoOut(int, string, string) : void
+  LocalIPAddress() : string
-  precedencebutton_Click(object, EventArgs) : void
-  precedencebutton2_Click(object, EventArgs) : void
-  prioritybutton_Click(object, EventArgs) : void
-  prioritybutton2_Click(object, EventArgs) : void
-  priorityTranslate(string) : int
-  setFunctionButtonColors() : void
-  setSipCfgParams() : void
-  showSplash() : void
-  startTrace() : void
-  textBox1_TextChanged(object, EventArgs) : void
-  textBox5_TextChanged(object, EventArgs) : void
-  timer1_Tick(object, EventArgs) : void
-  timer2_Tick(object, EventArgs) : void
-  timer3_Tick(object, EventArgs) : void
-  transferbutton_Click(object, EventArgs) : void
-  updateButtons(int) : void
-  userbutton_Click(object, EventArgs) : void
```

Figure 3-5 ASIP_GUI (Sheet 3 of 7)

Figure 3-5 ASIP_GUI (Sheet 4 of 7)

Figure 3-5 ASIP_GUI (Sheet 5 of 7)

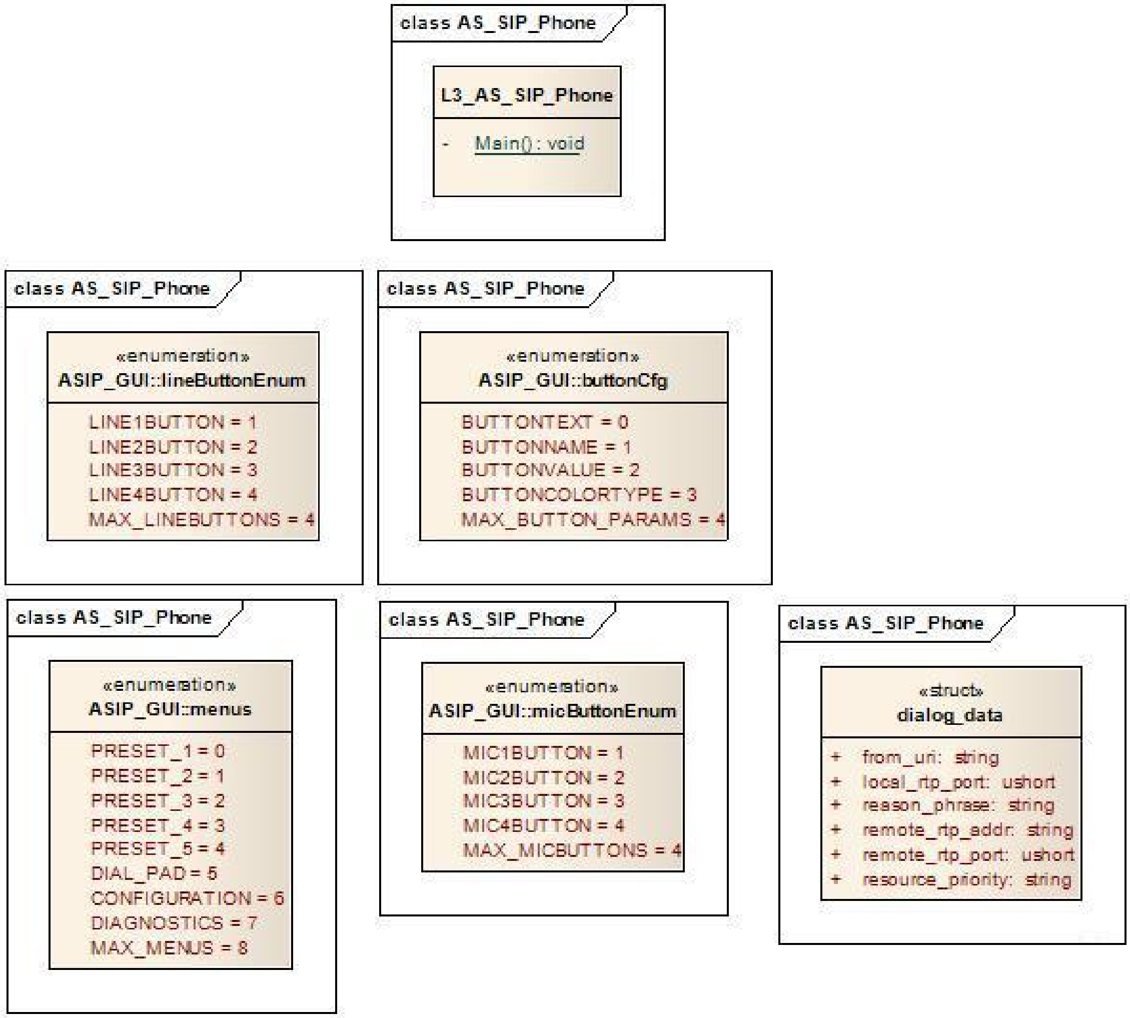


Figure 3-5 ASIP_GUI (Sheet 6 of 7)

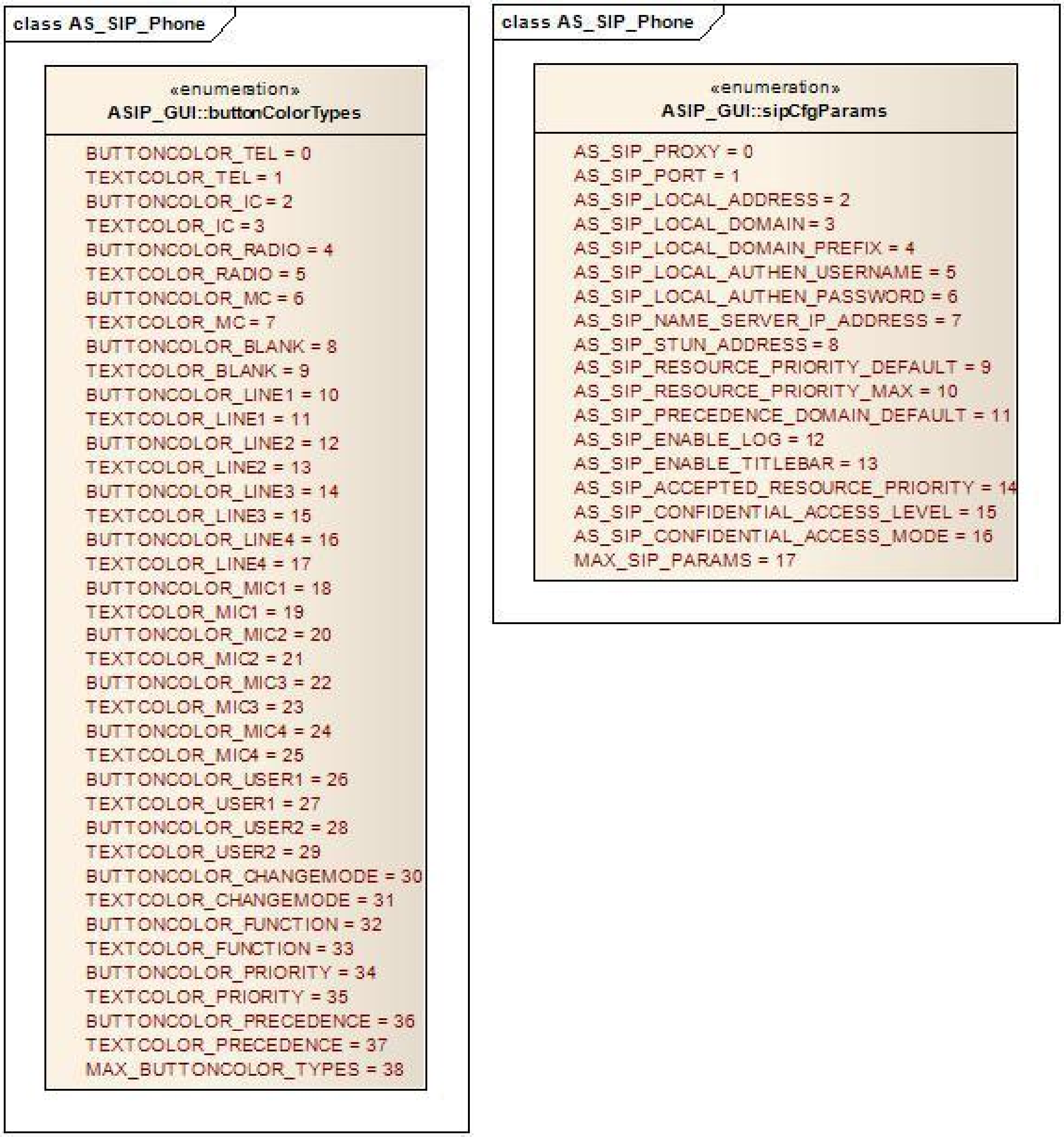


Figure 3-5 ASIP_GUI (Sheet 7 of 7)

3.1.2 Proof-of-Concept Software Development

3.1.2.1 Design Platform Decisions

The development environment was chosen for the following reasons:

1. .NET
   - Windows forms graphical application interface (API)
   - Data access framework
   - Managed code APIs allow for the C# GUI development to be decoupled from the SIP stack
   - Base Class Libraries (BCL) provide minimal set of .NET libraries for compact version
   - Framework Class Libraries (FCL) contains superset of .NET libraries - infrastructure for functionality expansion.
2. XP Embedded
   - Ability to choose only the components needed thereby reducing operating system footprint and also reducing attack potential
   - Allows for expansion potential of IP Communications Terminal functionality
   - Can satisfy processor intensive applications
3. C#
   - Object-oriented
   - GUI centric programming language
   - Microsoft development environment.

3.1.2.2 Design Platform Options

The following development environment options were considered, but not selected for the following reasons:

1. Java
   - Is similar to C#/.NET in look and feel
   - Has many open source applications developed

- Java however, is not for development organizations focused on Microsoft technology. Java provides a distinct and separate environment requiring some infrastructure adjustment.

2. Windows Mobile

- Is a compact operating system combined with a suite of basic applications for mobile devices based on the Microsoft Win32 API
- Is a "stripped-down" version of Windows running on a combination of RAM and flash resulting in less power
- Windows Mobile however, is not geared for a feature-rich IP end instrument – it is more for CPU intensive applications.

3. Linux

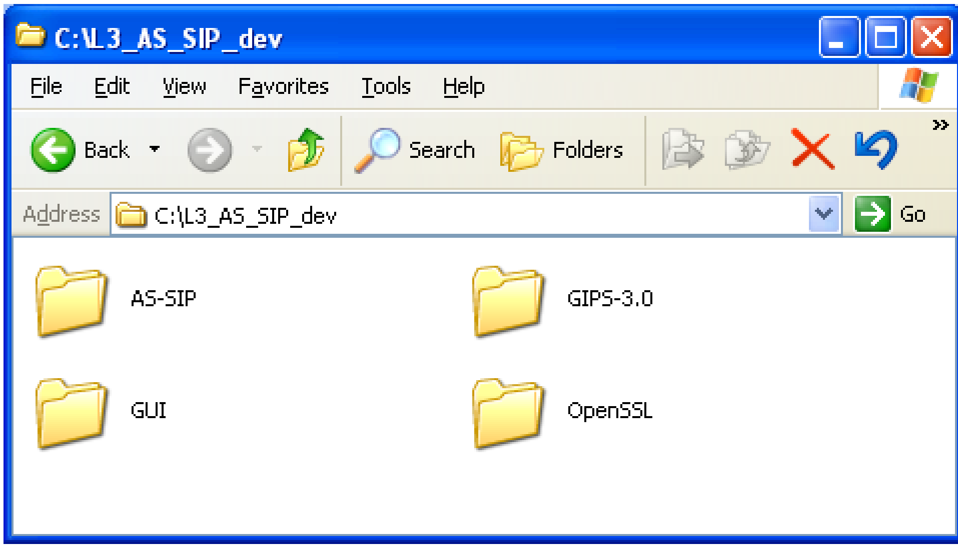
- Can be in compact form and provide an ideal environment for session-based applications
- Has wide variety of open-source SIP applications available
- Linux however, is not integrated with Microsoft Development Environment.

3.1.3 Proof-of-Concept: Development Environment

To create the development environment, the user is directed to AS-SIP, GUI, GIPS-3.0, and OpenSLL. All may be obtained from the DVD included with this document.

The Telesof*t* stack with modifications for AS-SIP should be placed in the AS-SIP directory (not located in the DVD included with this document) (Figure 3-6). The stack is integrated with GIPS voice engine 3.0 (use of the Telesoft stack requires a license).

Note: To build the code, Microsoft Visual Studio 2008 is used and must be installed on the development PC.



4

Figure 3-6 L3_AS_SIP Development Directory

3.1.4 Proof-of-Concept: Building AS-SIP Code

To bring up the AS-SIP IDE, in the GUI directory, run the file **L3_AS_SIP_Phone.csproj** (Figure 3-7). Note that the project file is highlighted in the right pane.

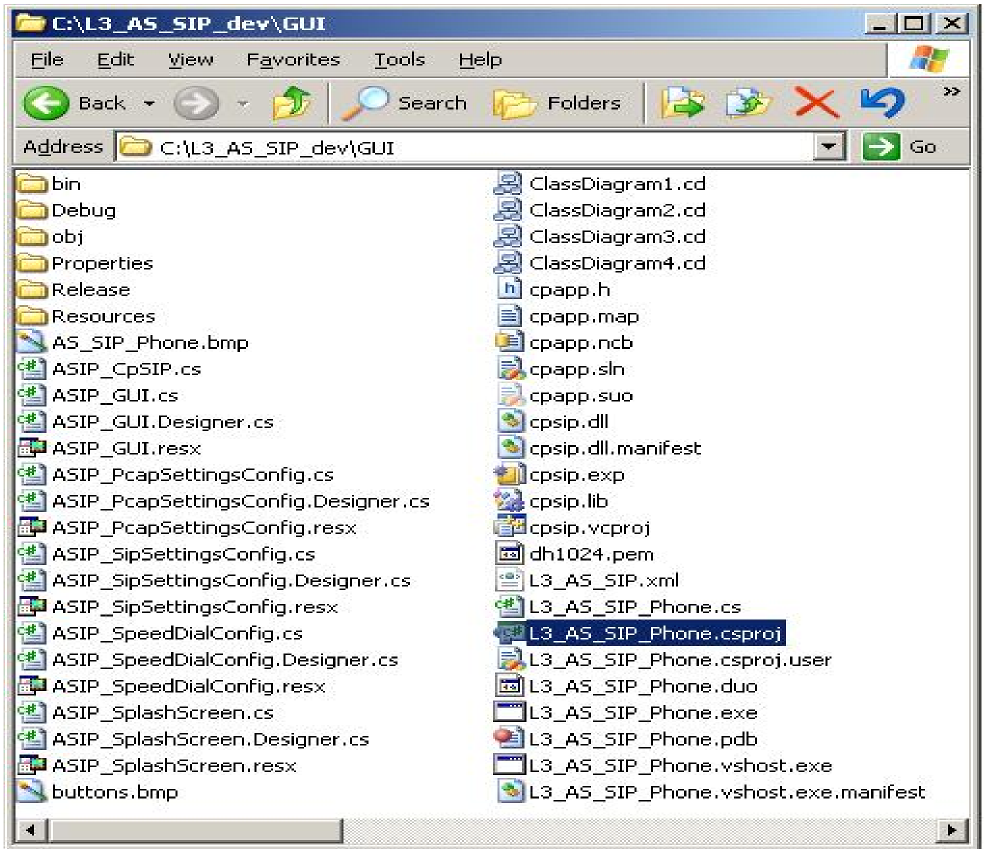


Figure 3-7 GUI Directory

Visual Studio should become active. After Visual Studio is activated, select the **Build** tab on the top toolbar (Figure 3-8), and select **build solution** from the **Build** pop-up and both **cpsip** and **L3_AS_SIP_Phone** are built. **Cpsip** can be built individually by selecting it from the solutions explorer. To build the dll only, select **Build cpcip.dll** from the **Build** pull-down menu. To build the **L3_AS_SIP_Phone.exe** only, select **L2_AS_SIP_Phone** project from the solutions explorer. Select **Build L3_AS_SIP_Phone** from the **Build** pull-down menu. **L3_AS_SIP_Phone.exe** is built and written to the GUI directory.

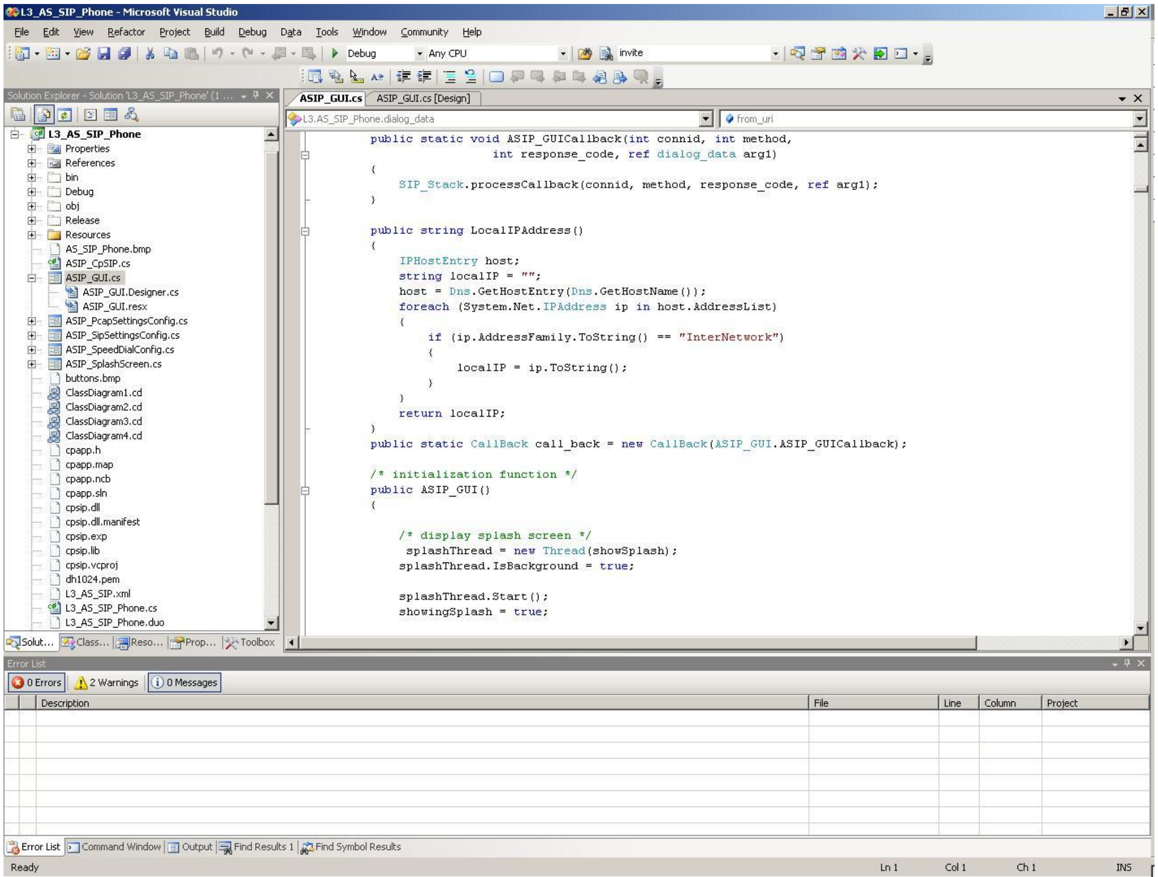


Figure 3-8 Microsoft Visual Studio

3.1.5 Proof-of-Concept: Running Code Locally

The Assured Services SIP code can be run as a softphone on the development PC. **Tamir.IPLib.dll, cpsip.dll** and the AS-SIP executable file **L3_AS_SIP_Phone.exe** must be in the current working directory.

Run L3_AS_SIP_Phone.exe and configure the system as detailed in paragraph 3.2, IP Communications Terminal: Configuration and Usage.

3.1.6 Proof-of-Concept: Installing Proof-of-Concept Hardware

The files shown in the L3_AS-SIP directory (Figure 3-9) are the minimum set of files needed to run the Proof-of-Concept code on the target hardware. Before executing, **dotnexfix3.5** must be run on the target system running XP Embedded.

The Configuration menu will be brought up by default when the application is executed. The device should be configured as described in paragraph 3.2, IP Communications Terminal: Configuration and Usage.

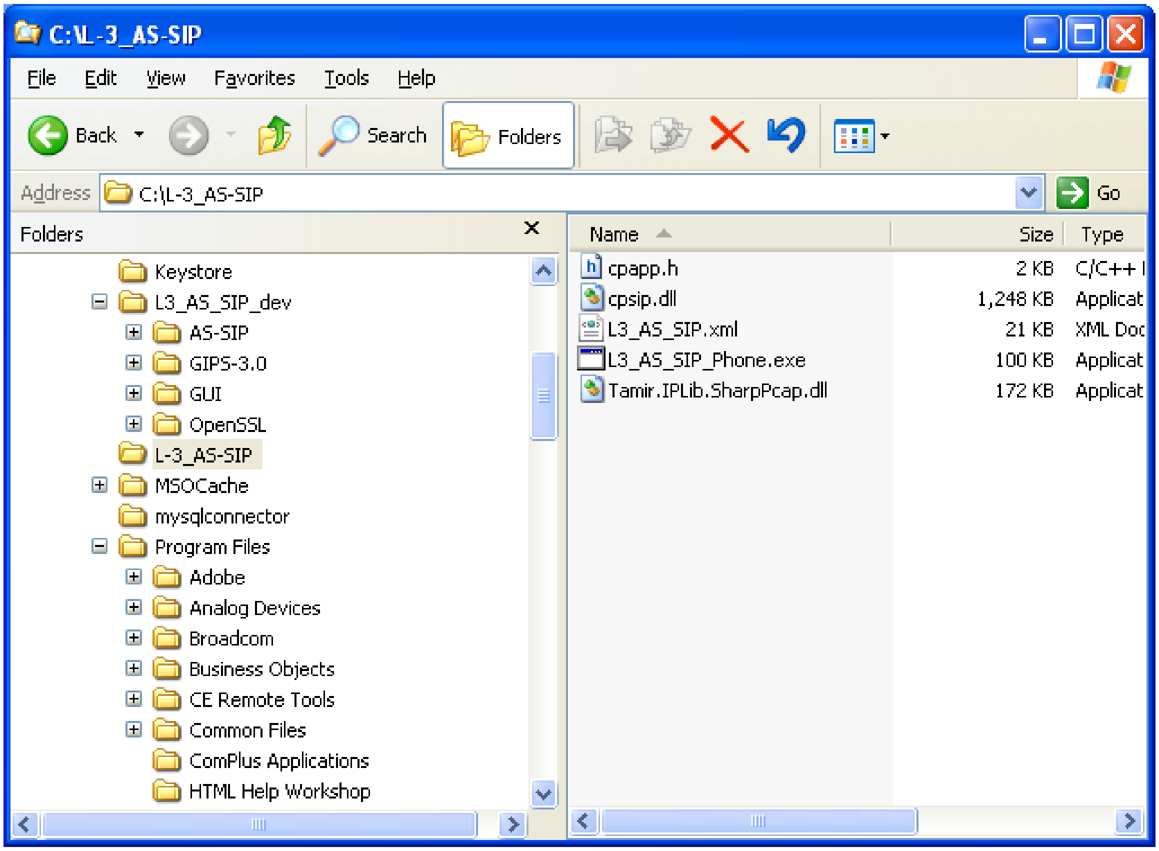


Figure 3-9 L-3_AS-SIP Directory

3.1.7 Proof-of-Concept Security

3.1.7.1 Device Access Security

At the user level, access to the device will be controlled by CAC Card or fingerprint scanner. A likely implementation would include user and application configuration and policy definition in a database which could be accessed based on biometric ID or CAC Card reading. Alternatively, configuration data can be stored on the CAC Card.

The current PoC implementation is exposed to potential risk by the use of readable XML stored on the local unit to establish connection with the proxy. It would be a better long-term solution to store this information in a secure database. User configurations left on a local device may be available to hackers on the IP network, particularly since XML is human-readable. The current implementation of the Proof-of-Concept allows for local saving of user passwords locally in an XML file. This is inadequate as a long term solution. The password for authentication should be entered on system initialization and not stored on the device.

It should be noted that in the current implementation, early media handling is enabled and not configurable. This behavior establishes voice path on INVITE. To some this may be considered a security concern. Voice path is established prior to acceptance by called party resulting in the ability of the calling party to hear the voice stream of the called party before the called party answers.

3.1.7.2 Session Access Security

The UCR references draft-hewett-sipping-cal-00 for session access security governed by the confidential access header. The confidential access level header provides a mechanism by which an end device assigns a security level for attempted session initiation.

Policy should be established regarding the levels assigned for each user/group and which mode should be employed – variable or fixed (the draft-hewett-sipping-cal-00 is discussed in detail in paragraph 3.1.9.2). It should be noted that currently most proxies, including the proxies with which the Proof-of-Concept was to be integrated, do not support draft-hewett-sipping-cal-00. It should also be noted that the current Proof-of-Concept implementation does not support reflected confidential access level as defined in draft-hewett-sipping-cal-00.

Also of note, end devices should handle the inability to initiate a session due to a confidential access level mismatch. In the case of confidential access mismatch, the proxy returns a 418 status code. The end device should handle the status code from the proxy and notify the user.

3.1.7.3 Classified/Unclassified Network Security

The future direction of IP Terminal development may require a second network interface (dual-homed) to support separate classified and unclassified networks.

IP Terminals may have the need to access classified networks at which time the device would need to disable the network connection to the unclassified network.

3.1.7.4 Remote Device Management

Device management is an area of needed research for security and for application maintenance. This is more often best achieved through a central device manager. Consideration should be given to expansion to support multiple device types and device platforms.

Consideration may be given to establishing policies which have application and application configuration removed from the device when a user is not logged in to the device. Policies should be established on a per device basis defining log-in durations. Certain devices may be sufficiently secure that no re-login interval needs to be set.

Removal of the application and configuration files will provide an added measure of security if the device is stolen or, in the case of mobile devices, lost.

The application should be loaded on login and removed requiring re-initialization when a network change is identified.

A central device management system of end points should provide:

1. Power-on password
2. Centrally enforced security policies
3. Disk encryption for end devices
4. Password recovery
5. Updates of application and data as needed
6. Management of group or individual configurations
7. Software distribution
8. Usage monitoring
9. Virus protection
10. Intrusion prevention
11. Unsolicited commercial email protection
12. Ability to encrypt data on device when device is loaded

3.1.7.5 General VoIP Security Recommendations

1. Keep voice network traffic hidden from data network users
2. Secure gateway limit system access to authenticated and approved users
3. Use Stateful Package Inspection (SPI) firewall and Network Address Translation (NAT) tools.

3.1.7.6 Transport Layer Security

Transport Layer Security (TLS) protocol is defined by RFC 5246 as a protocol that provides cryptographic security and data integrity for communications over TCP/IP networks (Figure 3-10).

The Session Initiation Protocol (SIP) Extension for Event State Publication describes a mechanism with which a presence user agent is able to publish presence information to a presence agent. Using the Presence Information Data Format (PIDF), each presence publication contains full state, regardless of how much of that information has actually changed since the previous update. As a consequence, updating a sizeable presence document with small changes bears a considerable overhead and is therefore inefficient. Especially with low bandwidth and high latency links, this can constitute a considerable burden to the system. This memo defines a solution that aids in reducing the impact of those constraints and increases transport efficiency by introducing a mechanism that allows for publication of partial presence information.

```
Client                                      Server

ClientHello             -------->
                                            ServerHello
                                               Certificate*
                                               ServerKeyExchange*
                                               CertificateRequest*
                        <--------              ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                -------->
                                              [ChangeCipherSpec]
                        <--------                       Finished
Application Data        <------->               Application Data
```

Figure 3-10 TLS Protocol Handshake (Reprinted from RFC 5246)

3.1.7.7 Secure Real-time Transport Protocol

RFC 3711: Encrypted RTP payload (not header), Master Key Identifier, and Authentication tag.

This document describes the Secure Real-time Transport Protocol (SRTP) [Figure 3-11], a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).

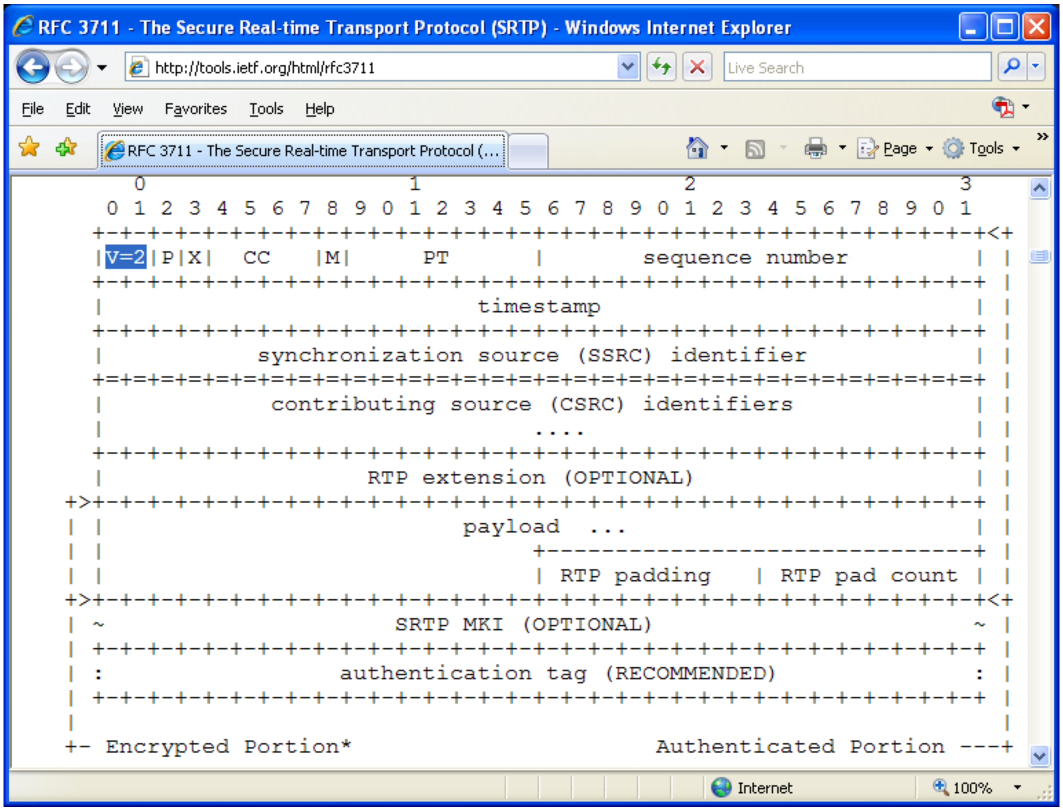


Figure 3-11 Secure Real-time Transport Protocol (SRTP)

3.1.8 Proof-of-Concept Assured Services SIP: An End Device Perspective

3.1.8.1 Reasons for AS-SIP

1. SIP Cluster

IP routing provides an inherent infrastructure for redundancy support. SIP servers can be clustered and with the use of Gratuitous ARP, server redundancy is easily achieved. The SIP end instrument sends and receives signals to a known proxy of FQDN or IP address handled through standard IP routing.

2. End-of-Life for Old Technology

The current technologies are being replaced in the corporate world with new technologies; making the old technology more expensive to purchase and maintain. SIP is mature enough to be widely deployed and continues to receive substantial funding for development with expanding use.

3. Newer Technology

Hardware devices supporting SIP are often smaller and lighter then the older technologies. Parts and devices are easily replaceable. With this also comes higher densities and reduced wire runs.

4. Simplicity/Flexibility of SIP

SIP is known for its flexibility and simplicity as a protocol. The control headers are in plain text allowing it to be human-readable. With the manufacturers focused on this new technology, enhancements are targeted at new products. The new technologies combine telephony and IP networks so a reduction is felt in wire runs, training and support. With this combined network, technologies like video can be added with minimum infrastructure cost.

3.1.8.2 AS-SIP Signaling – Multilevel Precedence and Preemption

The fundamental precept of Assured Services SIP is the ability to provide a mechanism for multilevel precedence and preemption.

1. Network Preemption

Network preemption on existing sessions and attempted sessions are controllable during high traffic resulting from crisis, network traffic surges, and network outages. In time of reduced bandwidth, end device sessions can be managed by gracefully tearing down lower priority sessions and allowing higher priority sessions to be established or to continue.

2. User Preemption

The MLPP is implemented via the resource priority header by Assured Services SIP. Local policy governs accepted priorities for users and end instruments. Graceful Assured Services initiated termination of sessions should be handled by end devices. The Assured Services end instrument should be capable of receiving and displaying preemption causes. Figure 3-12 (an excerpt from UCR 2008) lists disconnect cause values with corresponding description.

3. Preemption Cause Handling

Causes should be handled by the Assured Service End Instrument and a meaningful message corresponding to the description below should be displayed to the user.

Table 5.2.2-4. Disconnect Message Cause Value

DISCONNECT MESSAGE CAUSE VALUE	DESCRIPTION
8	Answered or Unanswered Call; Circuit is Not to be Reused
9	Answered or Unanswered Call; Circuit is to be Reused
46	Unavailable Resources; Precedence Call is Blocked with Equal or Higher Precedence Calls

Figure 3-12 Disconnect Message Cause Values

4. Preemption Tone Generation

End instruments should identify the priority of incoming sessions using at a minimum preemption tones (Figure 3-13). Preemption is applicable to all sessions initiated through all session functions (forward, transfer, hold, etc.).

Table 5.2.2-5. U.S. National Codepoints for Signal Values

SIGNAL VALUE	EXPLANATION	NORTH AMERICAN PRACTICE
9	Preemption tone is on	Precise tone is a continuous 440 Hz tone added to a 620 Hz tone
-	Precedence call alerting ringback tone on	Ringback tone (audible ringing tone) is a 440 Hz tone added to a 480 Hz tone repeated in a 1.64 s on, 0.36 s off pattern
66		Precedence call alerting 1.64 s on, 0.36 s off
Note – No signal value is assigned to "precedence call alerting ringback tone on" since the tone is always applied by the destination exchange. This ringback tone is as indicated in the table.		
Signal value (Octet 3) Bits 8 7 6 5 4 3 2 1 0 0 0 0 1 0 0 1 (9) Preemption tone 0 1 0 0 0 0 1 0 (66) Alerting on-pattern 2 (Special/priority alerting)		

Figure 3-13 Codepoints for Signal Values

3.1.9 SIP RFCs & Unified Capabilities Requirements 2008 (UCR 2008)

3.1.9.1 Proof-of-Concept: Supported RFCs

- RFC2327-SDP
- RFC2976- SIP INFO Method
- RFC3261- SIP
- RFC3262- Provisional Responses
- RFC3263- Locating SIP Servers
- RFC3264-Offer-Answer with SDP
- RFC3265- Event Notification
- RFC3325- P-Asserted Identity
- RFC3326- Reason Header
- RFC3428- Instant Messaging
- RFC3489- STUN
- RFC3515- SIP Refer Method
- RFC3550- RTP
- RFC 4028- Session Keep Alive
- draft-hewett-sipping-cal-00

3.1.9.2 RFCs of Importance

1. RFC 3261:

RFC 3261 details the SIP core signaling protocol definition.

This document describes Session Initiation Protocol (SIP), an application-layer control (signaling) [Figure 3-14] protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include internet telephone calls, multimedia distribution, and multimedia conferences.

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

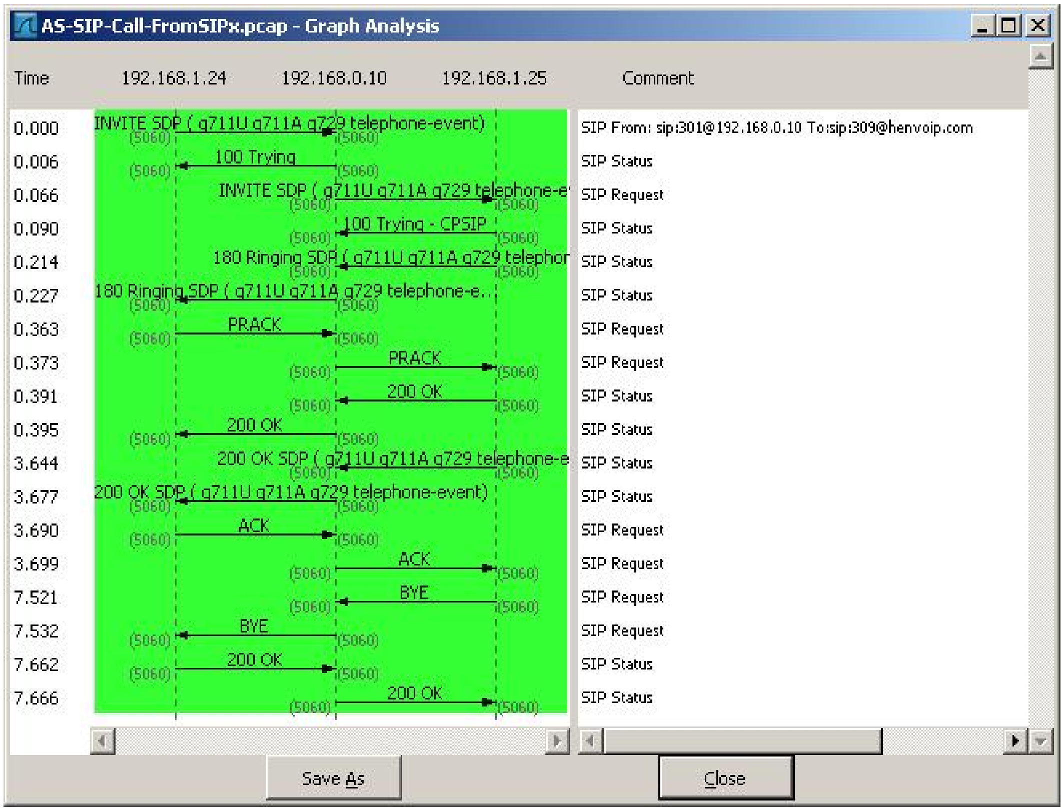


Figure 3-14 SIP Core Signaling

2. RFC 4412: RFC 4412 defines resource priority header format and the use of resource priorities for supporting multilevel precedence network conditions and user preemption.

This document defines two new Session Initiation Protocol (SIP) header fields [Figure 3-15] for communicating resource priority, namely, "Resource-Priority" and "Accept-Resource-Priority". The "Resource-Priority" header field can influence the behavior of SIP user agents (such as telephone gateways and IP telephones) and SIP proxies. It does not directly influence the forwarding behavior of IP routers.

In Figure 3-15, a protocol trace shows a AS-SIP precedence call in the domain dsn-000003 with resource priority 8 (flash override).

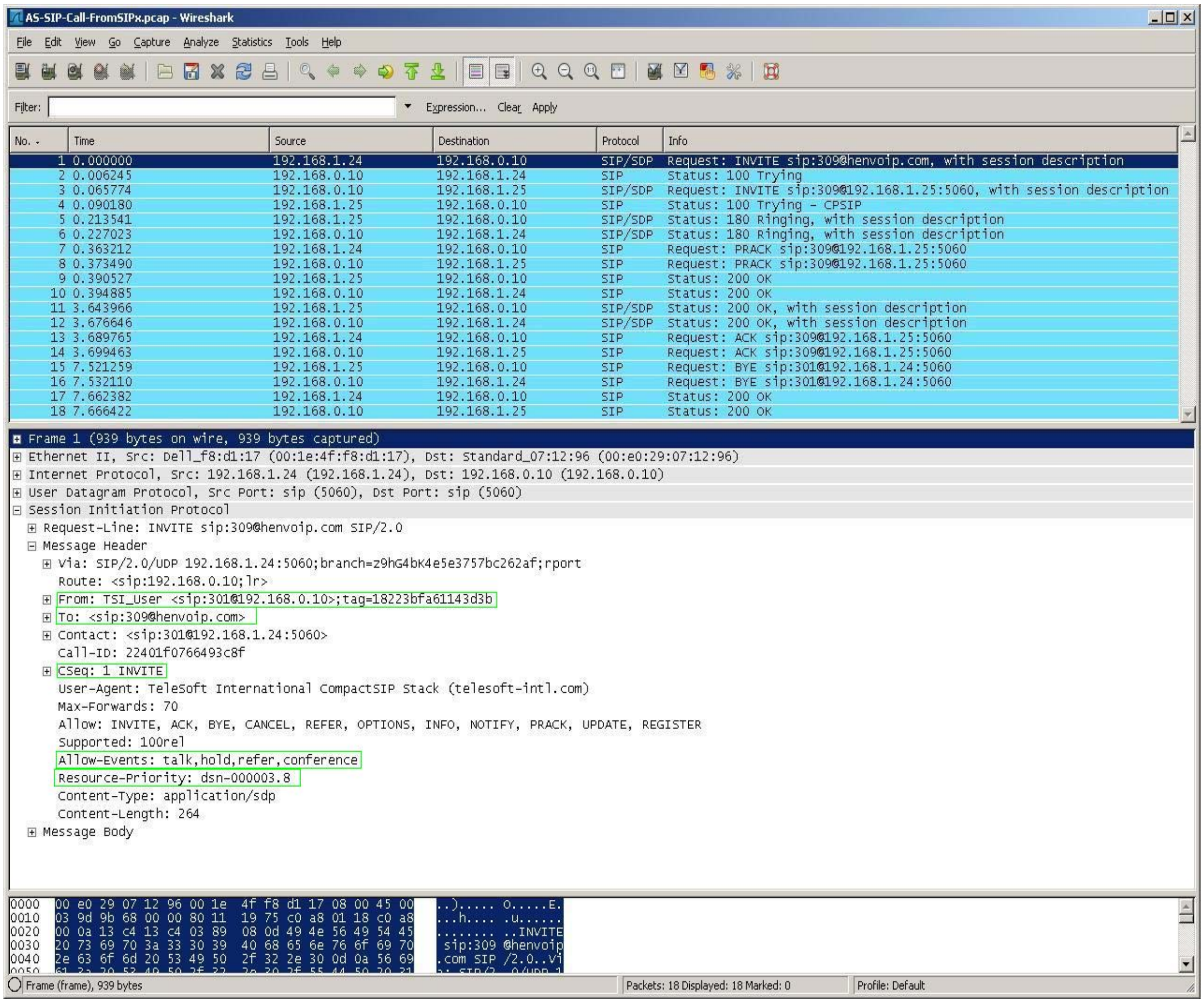


Figure 3-15 Resource Priorities Protocol Trace

a. Supported Priorities

Table 3-1 shows the supported resource priorities.

Table 3-1 Resource Priority Decimal Values

r-priority	CORRESPONDING DECIMAL VALUE
routine	0
priority	2
immediate	4
flash	6
flash-override	8

b. Precedence Domains

Assured Services SIP supports the dsn namespace and domains: 0-9. Precedence and preemption events are only applicable within the precedence domain.

SIP headers contain higher resource priority but are external to the controlled domain are to be ignored.

Example: dsn-000000.4

Precedence domain: dsn-000000
Resource priority: ‘immediate’

Within domain dsn-000000, this call has precedence over routine and priority calls.

3. RFC draft-hewett-sipping-cal-00

The Internet Engineering Task Force (IETF) RFC document *draft-hewett-sipping-cal-00* defines confidential access mode and level SIP headers. The end device sends access level (0-99) in the confidential-access-level header and mode in confidential-access-mode (fixed / negotiable). If the mode is set to fixed, sessions must have matched access level to establish sessions. If the mode is set to negotiable, the incoming access level must meet or exceed the local confidential access level.

The responsibility of the end device is to have a mechanism defined to set and allow confidential access levels and modes set in accordance with local policy. The UCR explicitly indicates that the signaling appliance is responsible for processing the confidential access header and responding to the initiating end device with the appropriate response code if the session cannot be initiated for confidential access reasons.

This specification defines a header for indicating the confidentiality level established between the involved parties.

confidential-access-level: (1*2DIGIT ; 0 to 99)
confidential-access-mode: (fixed / negotiable)

4. RFC 4411

RFC 4411 defines the extension of causes to support preemption signaling events.

This document defines two new Session Initiation Protocol (SIP) header fields for communicating resource priority, namely, "Resource-Priority" and "Accept-Resource-Priority". The "Resource-Priority" header field can influence the behavior of SIP user agents (such as telephone gateways and IP telephones) and SIP proxies. It does not directly influence the forwarding behavior of IP routers.

Cause Code	Reason-Text	Description
1	UA Preemption	A client initiated the preemption event.
2	Reserved Resources Preempted	The network initiated the preemption event.
3	Generic Preemption	Response to UA if it is desirable to hide the preemption reason from the client.
4	Non-IP Preemption	Preemption event received external to the IP network.

5. RFC 3960

This document describes how to manage early media in the Session Initiation Protocol (SIP) using two models: the gateway model and the application server_model. It also describes the inputs one needs to consider in defining local policies for ringing tone generation.

Empty INVITE

Voice path is established on INVITE signal.

No Negotiation of Voice Parameters on AS-SIP INVITE:

- Voice path established on INVITE
- Session description defined by caller
- No Offer/Answer Model for priority calls
- If empty INVITE (no SDP with INVITE), then SDP in 200 OK from answerer is used

Ringing Tones: Generated Locally

- Tones generated by calling device
- Frequency & Duration defined for preemption events (see Preemption Tone Generation)

3.1.9.3 AS-SIP Areas of Concern

1. Interoperability with SIP Signaling Appliances and End Instruments -

All devices today (expect for the PoC) don't support AS-SIP. Many devices that will be encountered will not support AS-SIP in the near future. It is not just phones that need to be changed, but also other components like Media Gateways and Border Controllers that will need to have AS-SIP added to them.

2. Management and Control of Local Policies for Assured Service - There is the need to manage local policies for assured services. No method of doing this has been seen by L-3 Henschel to date.

3. Under-Defined End Instrument Requirements - The requirements for the end devices are coming but at this time they have not been written and approved. This process should be starting in the near future and will take close to a year to complete. At that time the Navy will have the ability to purchase any AS-SIP phone and use it with any AS-SIP enabled LCS.

4. Verification and Test Maturity – End device specifications using AS-SIP have yet to be written. Verification and testing will need to be done in accordance with the specification.

5. Early Media - It should be noted that in the current implementation, early media handling is enabled and is not configurable. This behavior establishes voice path on INVITE. To some this may be considered a privacy concern and it may be desirable to make a settable configuration parameter.

3.2 PoC IP Communications Terminal: Configuration and Usage

The currently loaded PoC configuration is written to L3_AS_SIP.xml.

3.2.1 Basic Configuration

Configuration of the PoC should be done using the configuration menu in the foreground when the application is initiated (Figure 3-16). The configuration is stored in the editable XML file L3_AS_SIP.xml. It is recommended that configuration is done using the configuration menu in the application.

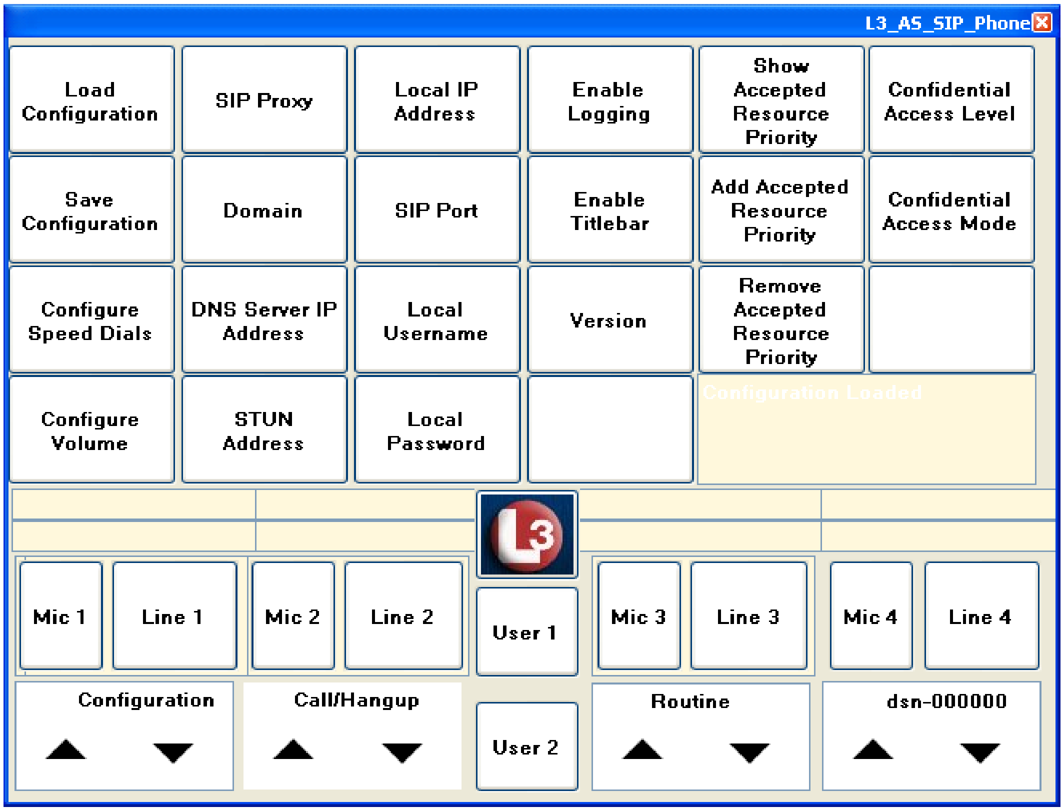
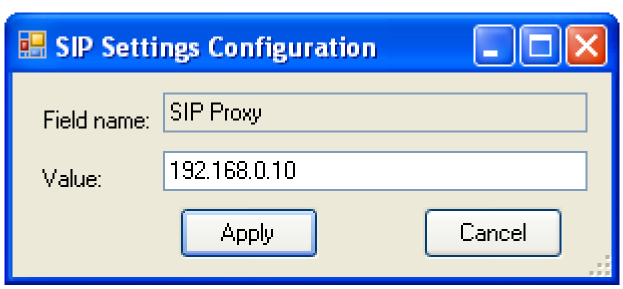


Figure 3-16 Proof-of-Concept Configuration Menu

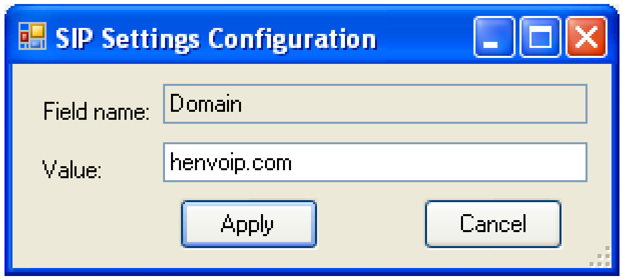
3.2.1.1 Basic Configuration Procedure

Steps 1 thru 6 illustrate a basic configuration procedure. For more information on additional configuration menu buttons, refer to Table 3-2.

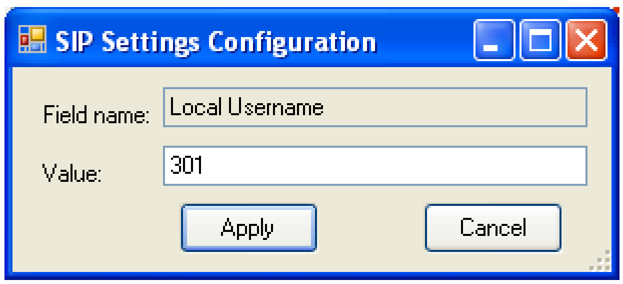
1. Enter the SIP Proxy by pressing the **SIP Proxy** button (Figure 3-16). Use the on-screen keyboard to enter the proxy IP address or FQDN in the *SIP Settings Configuration* dialogue box. Press **Apply**.



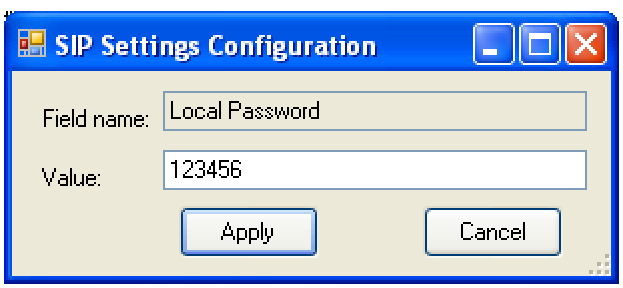
2. Enter the Domain by pressing the **Domain** button. Use the on-screen keyboard to enter the domain in the *SIP Settings Configuration* dialogue box. Press **Apply**.



3. Enter the User Name by pressing the **Local Username** button. Use the on-screen keyboard to enter the device username in the *SIP Settings Configuration* dialogue box. Press **Apply**.



4. Enter the User Name by pressing the L**ocal Password** button. Use the on-screen keyboard to enter the device password in the *SIP Settings Configuration* dialogue box. Press **Apply**.



5. Save the configuration by pressing the **Save Configuration** button.

6. Load the configuration by pressing the **Load Configuration** button. The system will reinitialize with the new settings.

Table 3-2 Additional Configuration Menu Buttons

Menu Button	Description
Configure Volume	Adjusts speaker volume level
DNS Server IP Address	Sets IP address of DNS Server
STUN Address	Sets IP address of STUN Server
Local Username	Sets Phone Number of local unit
Local Password	Sets Password of local unit
Local IP Address	Shows the current IP address of the PoC
SIP Proxy	Set SIP proxy IP address
Domain	Set domain name
Enable Logging	Enables logging
Enable Titlebar	Enables Titlebar
Version	Shows Software Version
Show Accepted Resource Priority	Shows the list of resource priorities accepted by the end device
Add Accepted Resource Priority	Adds a resource priority to the list of resource priorities accepted by the end device. The priority and precedence to be added is identified by the labeled priority and precedence buttons in the lower right corner of the screen.
Remove Accepted Resource Priority	Removes a resource priority to the list of resource priorities accepted by the end device. The priority and precedence to be removed is identified by the labeled priority and precedence buttons in the lower right corner of the screen.

Table 3-2 Additional Configuration Menu Buttons – Continued

Menu Button	Description
Confidential Access Level	1*2DIGIT ; 0 to 99 SEMI access-mode; sets Confidential access level
Confidential Access Mode	Fixed or negotiable; sets confidential access mode

3.2.1.2 Setting Speed Dials

Steps 1 thru 5 illustrate the procedure for setting the Speed Dial configuration at the Configuration Menu (Figure 3-17).

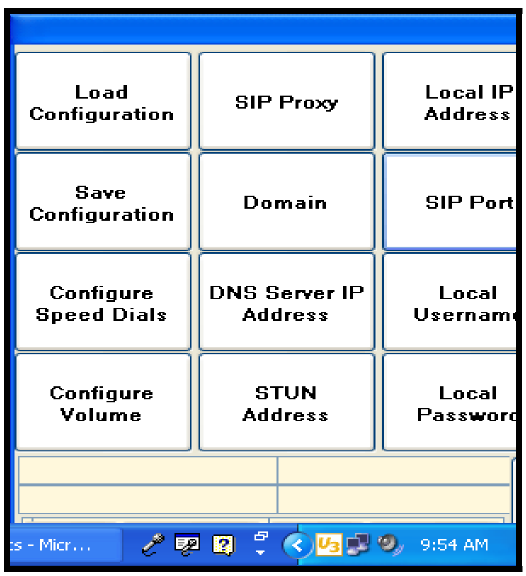
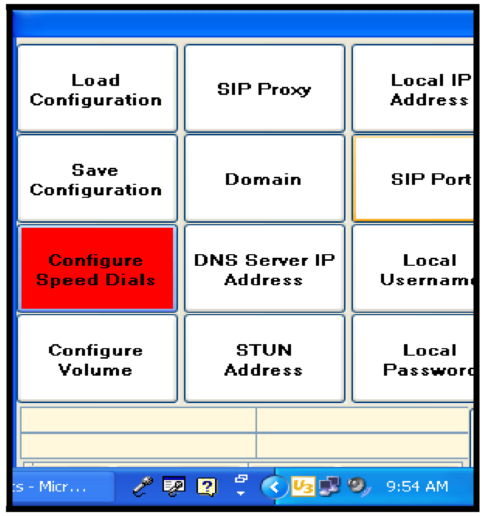


Figure 3-17 Configure Speed Dials Button on the Configuration Menu

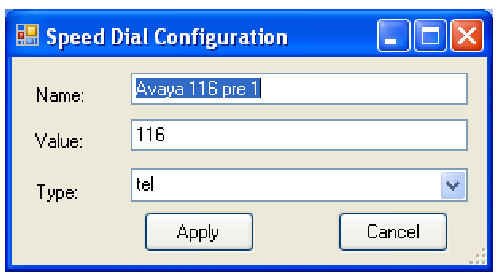
1. Configure speed dial settings by selecting the **Configure Speed Dials** menu button.

2. Observe that the **Configure Speed Dials** button background turns to red.



3. Navigate to desired preset button.

4. Press the button and observe the *Speed Dial Configuration* window appears.



5. Using the on-screen keyboard, enter the **Name:**, **Value:**, and **Type:** fields, and press **Apply**.

6. Press **Configure Speed Dials**, and observe the background returns to the default.

7. Save the configuration.

Note: The configuration must be saved in order for the system to retain it.

3.2.2 Using the L3_AS_SIP_Phone

1. Starting L3_AS_SIP_Phone

To start L3_AS_SIP_Phone, click on the L3_AS_SIP_Phone.exe file (note that the .exe extension in L3_AS_SIP_Phone.exe may not be displayed).

2. Exiting L3_AS_SIP_Phone

Exit L3_AS_SIP_Phone by clicking the L3 image in the lower center of each menu screen (Figure 3-18).

3. Screens

L3 AS-SIP Phone screens can be navigated using the Mode button in the lower left corner of the screen (Figure 3-19). Each screen maintains the bottom button set which includes:

1. Mode
2. Call Function
3. Priority
4. Precedence Domain
5. Four line buttons with corresponding Information boxes and microphone toggle button.

4. Modes:

1. Five **Preset** Modes
2. **Dial Pad** Mode
3. **Diagnostics** Mode
4. **Configuration** Mode

5. Call Functions

1. **Call/Hangup**
2. **Hold/Resume**
3. **Forward en/dis**
4. **Transfer**
5. **Redial**
6. **Messages**

3.2.2.1 Preset Modes

Preset modes are set in the XML config file displaying text to users mapped to phone numbers sent to SIP Proxy. To place a call in the preset mode:

1. Select function (**Call/Hangup** is the default).
2. Select line (press line button, such as **Line 1** – observe button border darkened for selected line).
3. Select **Preset** button. The number associated with that button will be sent to the proxy.

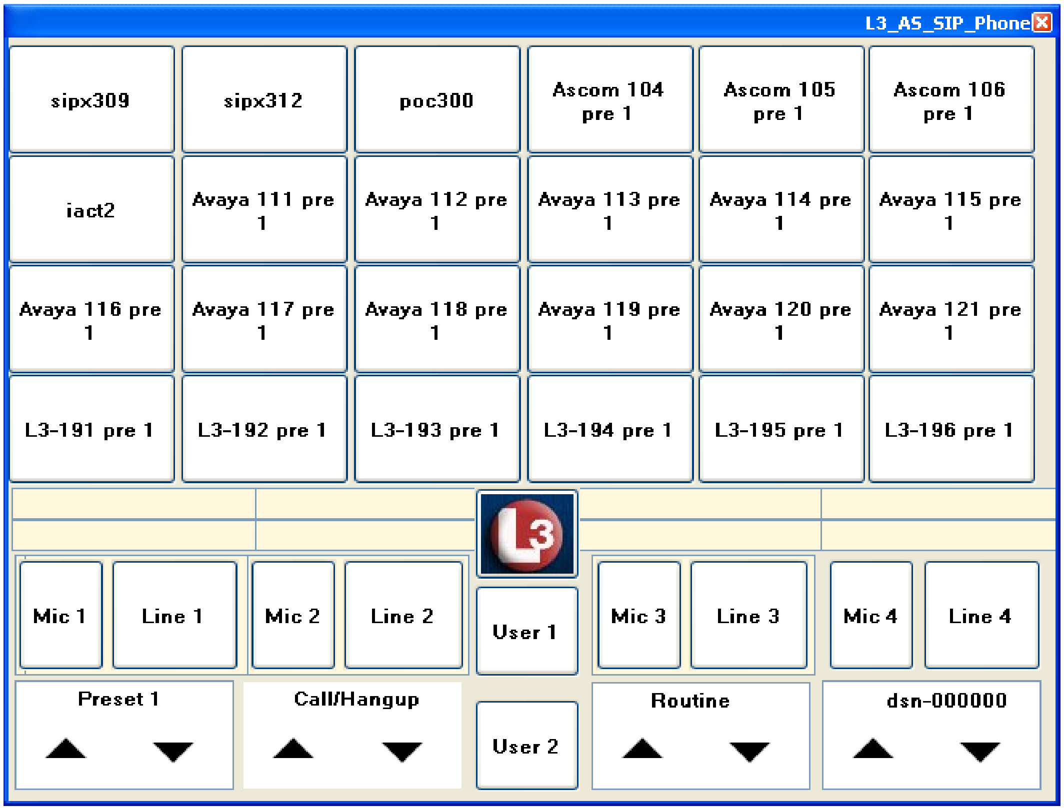


Figure 3-18 L3_AS_SIP_Phone GUI Sample Preset Menu

3.2.2.2 Dial Pad Mode

The Dial Pad Screen is displayed after hitting the **Mode** button until **Dial Pad** is displayed on the **Mode** button. To place a call in the dial pad mode:

1. Select function (**Call/Hangup** is the default).
2. Select line (press line button, such as **Line 1** – observe button border darkened for selected line).
3. Press number keypad for number to be called.

4. Observe number in corresponding line information box.
5. Initiate call by pressing **Call** button (Figure 3-19, second button from right on top line of dial pad).

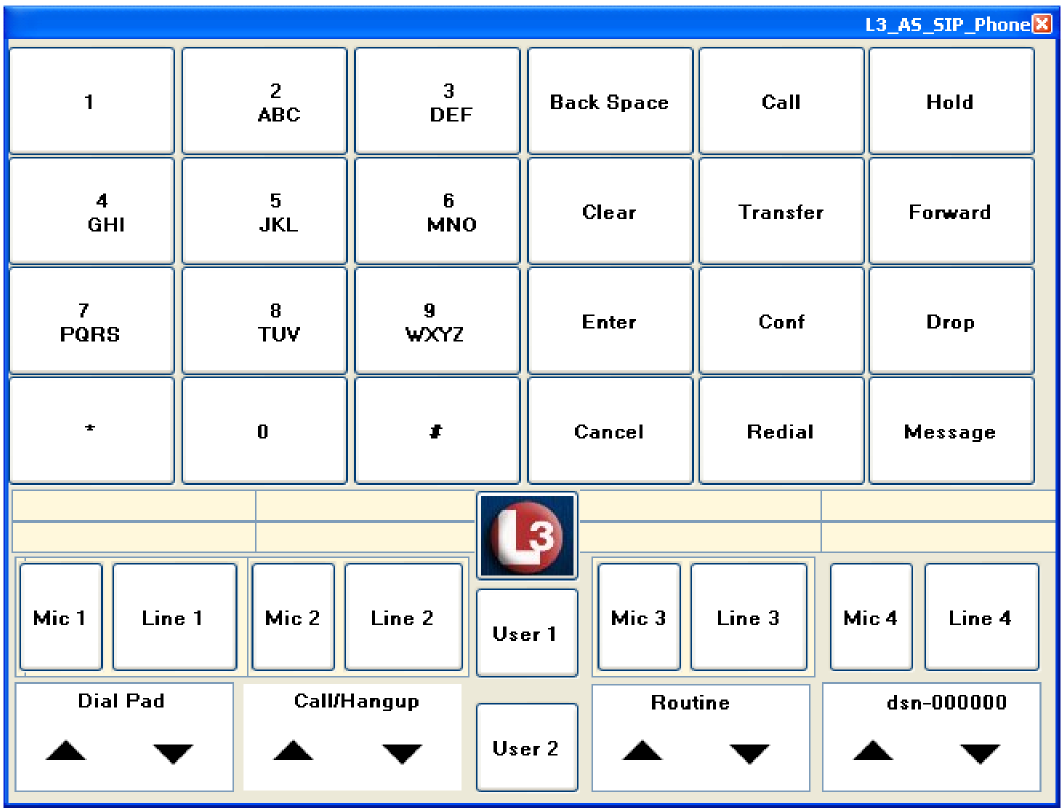


Figure 3-19 L3_AS_SIP_Phone GUI Sample Dial Pad Menu

3.2.3 Diagnostics

To enable SIP protocol tracing, press the **Start Trace** button on the Diagnostic Menu screen (Figure 3-20).

The options of network cards to trace are displayed. Select the network card to trace. Proceed with events to be traced.

Turn off tracing by selecting the **End Trace** button. The file **diagnostics_output.pcap** will be generated in the default directory. The **pcap** file can be off-loaded and interpreted by a protocol analyzer. The file is overwritten each time trace is enabled.

Note: Trace files grow quickly; **Start Trace** should only be enabled when the need is present and turned off after the call is completed.

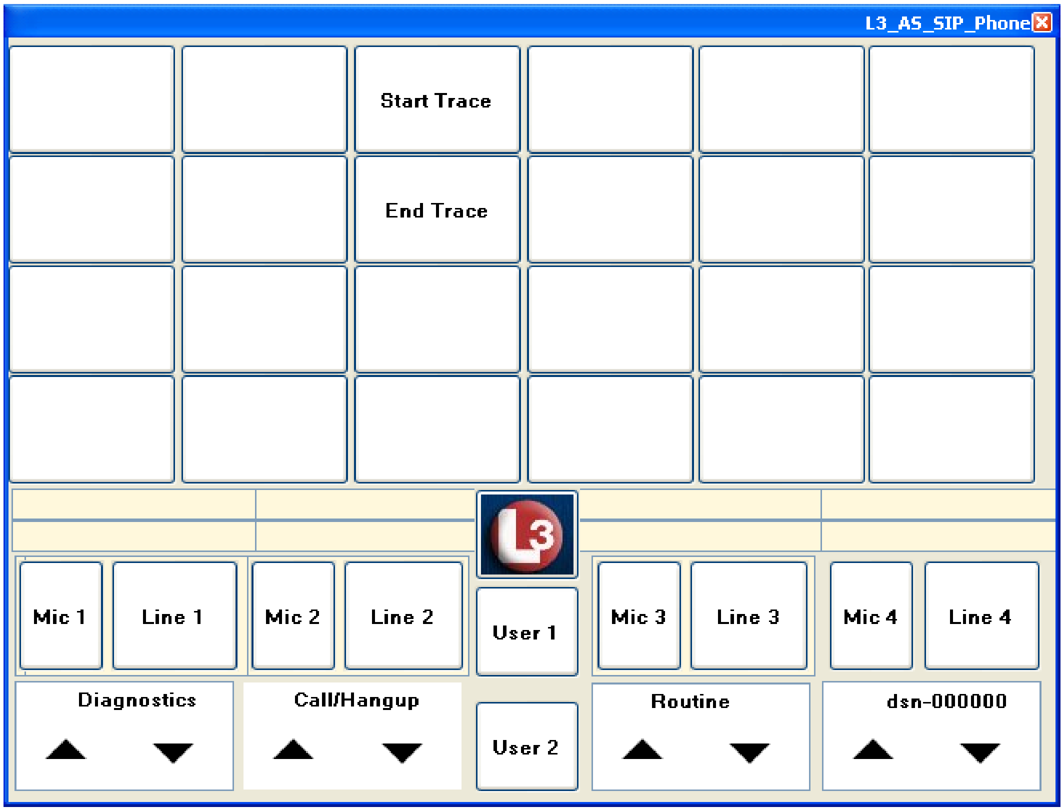


Figure 3-20 Diagnostic Menu Screen

3.2.3.1 Call Functions

The line button on the line corresponding to the inbound call will flash **RING** in red. Press the line button and the incoming call will become active and the line will indicate this by changing the line button green and relabeling **Active**.

3.2.3.2 Call/Hangup

To place a call, perform the following:

1. Select mode **Call/Hangup**.
2. Select **Line** (observe darkened button border).
3. Press **Preset** or **Dial Pad** numbers (see paragraphs 3.2.2.1 and 3.2.2.2).
4. **Dial** will appear in line button with an orange background until call is active or terminated.
5. Voice path will be established when called party answers and line button text reads **Active** with a green background.
6. To cancel call, press line button and the line number text will be displayed in the line button.

To terminate a call:

1. Select mode **Call/Hangup**.
2. Select **Line** (observe darkened button border).
3. Line button will no longer indicate **Active** and the button text will indicate the line number. Voice path will be torn down.

3.2.3.3 Hold/Resume

To place a call on hold, perform the following:

1. Select mode **Hold/Resume**
2. Select **Line** (observe darkened button border).
3. Observe line button, **HOLD** will appear in line button with red background.
4. Voice path is suspended

To resume a call on hold:

1. Select mode **Hold/Resume**
2. Select **Line** (observe darkened border)
3. Voice path will be established when called party answers and line button text will read **Active** with a green background.

3.2.3.4 Forward Enable/Disable

To forward calls, perform the following:

1. Select mode **Forward en/dis.**
2. Select **Line** (observe darkened button border).
3. Line corresponding information text box will instruct user to input forwarding number. If in **Preset** mode, select **Preset** button. If in **Dial Pad** mode, enter number, then press **Forward**.
4. Forwarding message and address is displayed for corresponding line.

To cancel call forwarding,

1. Select Mode **Forward en/dis.**
2. Select **Line** (observe darkened button border).
3. Voice path will be established when called party answers and line button text will read **Active** with a green background.
4. Line button text will indicate the line number.

3.2.3.5 Transfer

To transfer calls, perform the following:

1. Select mode **Transfer**.
2. Select **Line** (observe darkened button border).

3 Line corresponding information text box will instruct user to input transfer number. If in **Preset** mode, select **Preset** button. If in **Dial Pad** mode, enter number, the press forward.
4. Transfer message and address is displayed for corresponding line.
5. Corresponding line button and information boxes are reset.

3.2.3.6 Redial

To redial number, perform the following:

1. Select mode **Redial**.
2. Select Line (observe darkened button border).
3. Line corresponding information text box will indicate the redialed number.
4. **Dial** will appear in line button with orange background until call is active or terminated.
5. Voice path will be established when called party answers and line button text reads **Active** with a green background.

3.2.4 Resource Priority

Outgoing calls will include a resource priority header with value indicated in Table 3-3. The resource priority button can be pressed and the priorities are displayed sequentially in priority order. When the call is initiated, the priority indicated by this button will be placed in the resource priority header (refer to Figure 3-21).

Table 3-3 Resource Priority Decimal Values

r-priority	CORRESPONDING DECIMAL VALUE
routine	0
priority	2
immediate	4
flash	6
flash-override	8

3.2.5 Precedence Domain

Outgoing calls will include precedence domain in the resource priority header. The precedence domain button can be pressed and the precedence domains are displayed sequentially. The default is dsn-000000. When the call is initiated, the precedence domain indicated by this button will be placed in the resource priority header as seen in Figure 3-21.

In the protocol trace, the SIP Message Header contains a **Resource-Priority:** header of **dsn-000000.0**. This corresponds to the default precedence domain (dsn-000000) and routine priority call (.0).

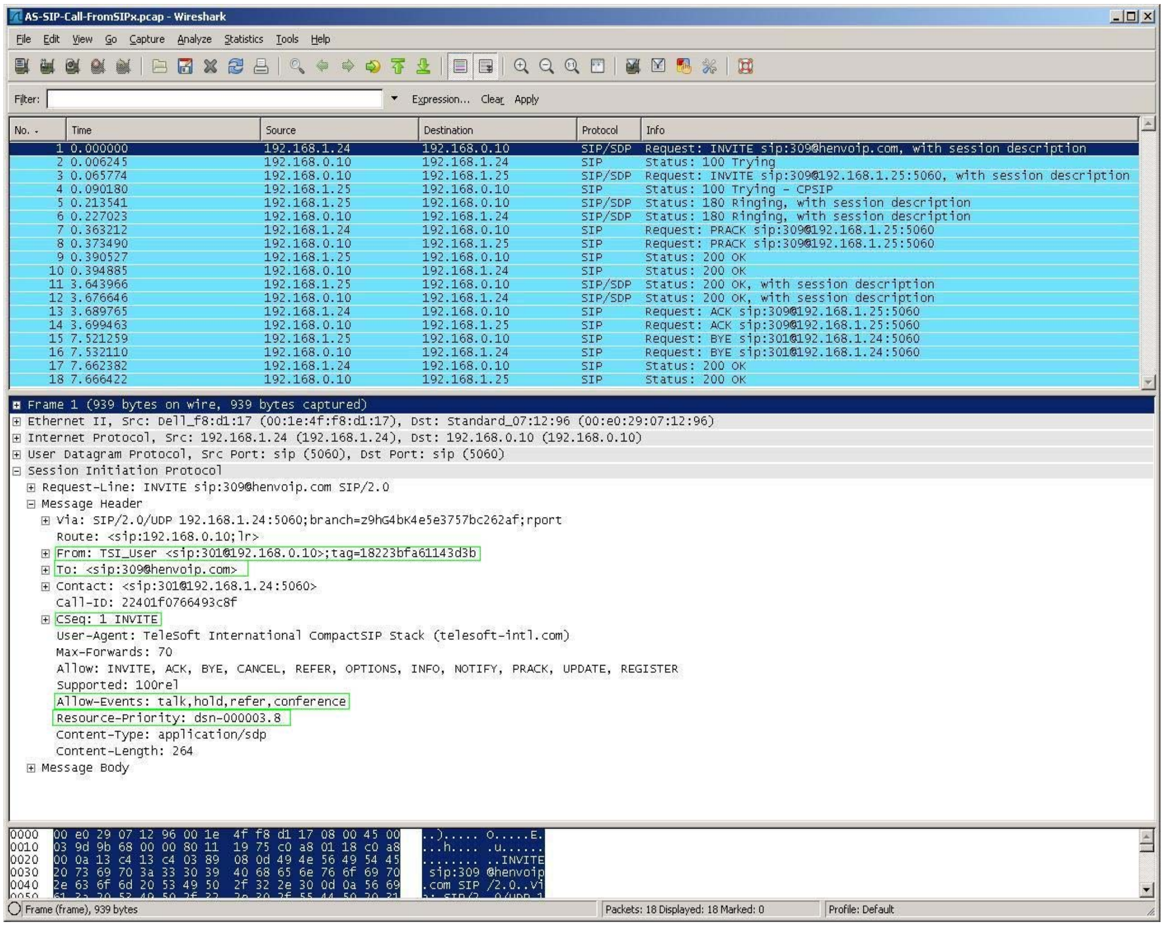
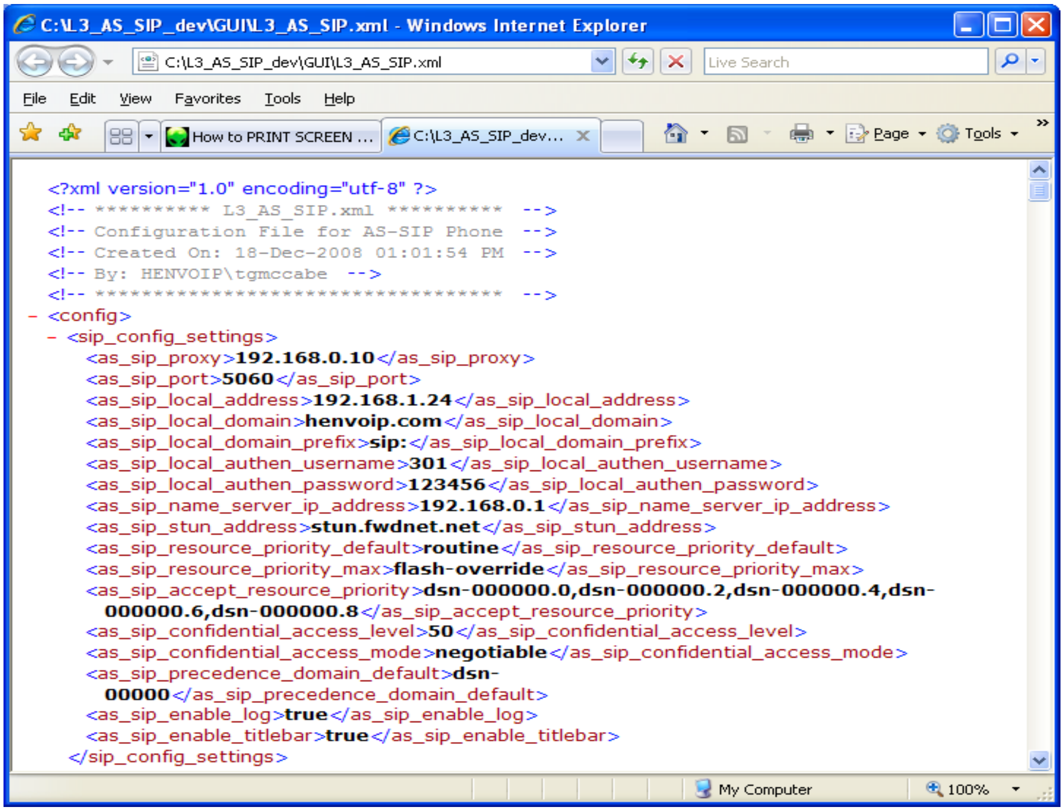


Figure 3-21 L3_AS_SIP_Phone Resource Priority Protocol Trace

3.2.6 Configuring L3_AS_SIP_Phone Menus and Buttons

This paragraph describes configuring buttons and menus for the end instrument.

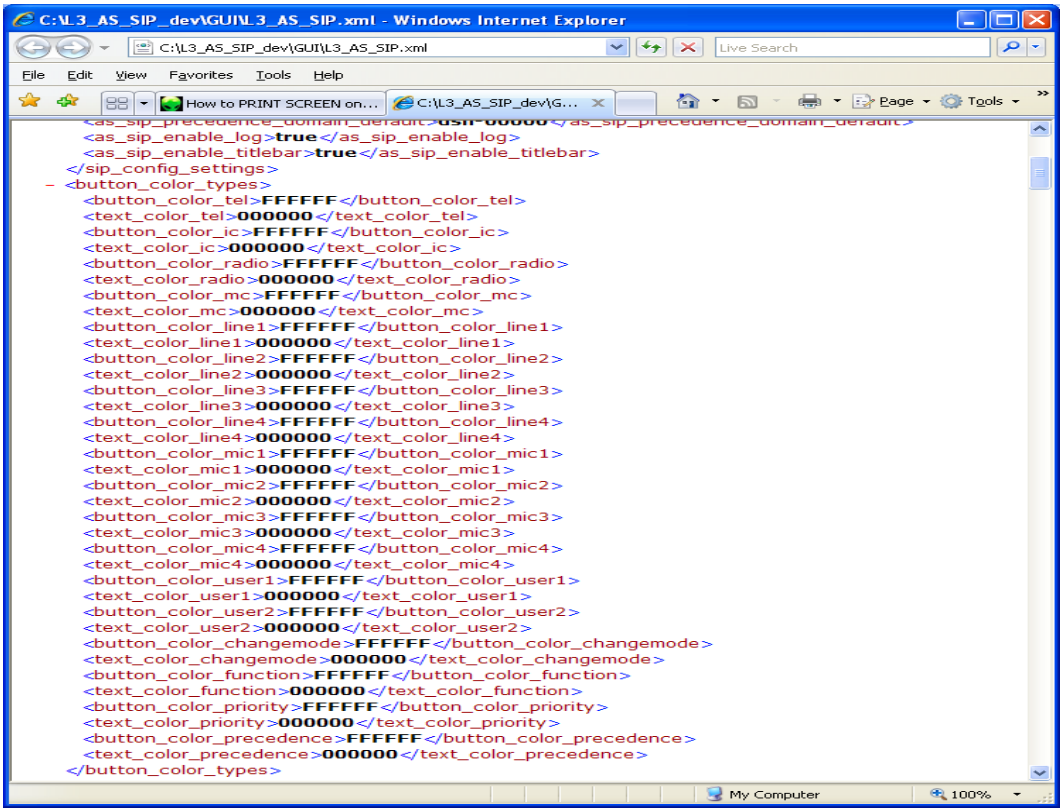



```xml
<?xml version="1.0" encoding="utf-8" ?>
<!-- ********** L3_AS_SIP.xml ********** -->
<!-- Configuration File for AS-SIP Phone -->
<!-- Created On: 18-Dec-2008 01:01:54 PM -->
<!-- By: HENVOIP\tgmccabe -->
<!-- *********************************** -->
- <config>
  - <sip_config_settings>
      <as_sip_proxy>192.168.0.10</as_sip_proxy>
      <as_sip_port>5060</as_sip_port>
      <as_sip_local_address>192.168.1.24</as_sip_local_address>
      <as_sip_local_domain>henvoip.com</as_sip_local_domain>
      <as_sip_local_domain_prefix>sip:</as_sip_local_domain_prefix>
      <as_sip_local_authen_username>301</as_sip_local_authen_username>
      <as_sip_local_authen_password>123456</as_sip_local_authen_password>
      <as_sip_name_server_ip_address>192.168.0.1</as_sip_name_server_ip_address>
      <as_sip_stun_address>stun.fwdnet.net</as_sip_stun_address>
      <as_sip_resource_priority_default>routine</as_sip_resource_priority_default>
      <as_sip_resource_priority_max>flash-override</as_sip_resource_priority_max>
      <as_sip_accept_resource_priority>dsn-000000.0,dsn-000000.2,dsn-000000.4,dsn-
        000000.6,dsn-000000.8</as_sip_accept_resource_priority>
      <as_sip_confidential_access_level>50</as_sip_confidential_access_level>
      <as_sip_confidential_access_mode>negotiable</as_sip_confidential_access_mode>
      <as_sip_precedence_domain_default>dsn-
        00000</as_sip_precedence_domain_default>
      <as_sip_enable_log>true</as_sip_enable_log>
      <as_sip_enable_titlebar>true</as_sip_enable_titlebar>
    </sip_config_settings>
```


Figure 3-22 Configuration File for L3_AS_SIP_Phone XML

3.2.6.1 Configuring Button Settings

Button settings are defined in L3_AS_SIP.xml (Figure 3-22 thru Figure 3-24). The settings define what is displayed to the user on end-instrument buttons and the values which are sent by the application to the SIP signaling appliance.




```
    <as_sip_precedence_domain_default>dsn-00000</as_sip_precedence_domain_default>
    <as_sip_enable_log>true</as_sip_enable_log>
    <as_sip_enable_titlebar>true</as_sip_enable_titlebar>
  </sip_config_settings>
- <button_color_types>
    <button_color_tel>FFFFFF</button_color_tel>
    <text_color_tel>000000</text_color_tel>
    <button_color_ic>FFFFFF</button_color_ic>
    <text_color_ic>000000</text_color_ic>
    <button_color_radio>FFFFFF</button_color_radio>
    <text_color_radio>000000</text_color_radio>
    <button_color_mc>FFFFFF</button_color_mc>
    <text_color_mc>000000</text_color_mc>
    <button_color_line1>FFFFFF</button_color_line1>
    <text_color_line1>000000</text_color_line1>
    <button_color_line2>FFFFFF</button_color_line2>
    <text_color_line2>000000</text_color_line2>
    <button_color_line3>FFFFFF</button_color_line3>
    <text_color_line3>000000</text_color_line3>
    <button_color_line4>FFFFFF</button_color_line4>
    <text_color_line4>000000</text_color_line4>
    <button_color_mic1>FFFFFF</button_color_mic1>
    <text_color_mic1>000000</text_color_mic1>
    <button_color_mic2>FFFFFF</button_color_mic2>
    <text_color_mic2>000000</text_color_mic2>
    <button_color_mic3>FFFFFF</button_color_mic3>
    <text_color_mic3>000000</text_color_mic3>
    <button_color_mic4>FFFFFF</button_color_mic4>
    <text_color_mic4>000000</text_color_mic4>
    <button_color_user1>FFFFFF</button_color_user1>
    <text_color_user1>000000</text_color_user1>
    <button_color_user2>FFFFFF</button_color_user2>
    <text_color_user2>000000</text_color_user2>
    <button_color_changemode>FFFFFF</button_color_changemode>
    <text_color_changemode>000000</text_color_changemode>
    <button_color_function>FFFFFF</button_color_function>
    <text_color_function>000000</text_color_function>
    <button_color_priority>FFFFFF</button_color_priority>
    <text_color_priority>000000</text_color_priority>
    <button_color_precedence>FFFFFF</button_color_precedence>
    <text_color_precedence>000000</text_color_precedence>
  </button_color_types>
```


Figure 3-23 Button Speed Dial Settings XML

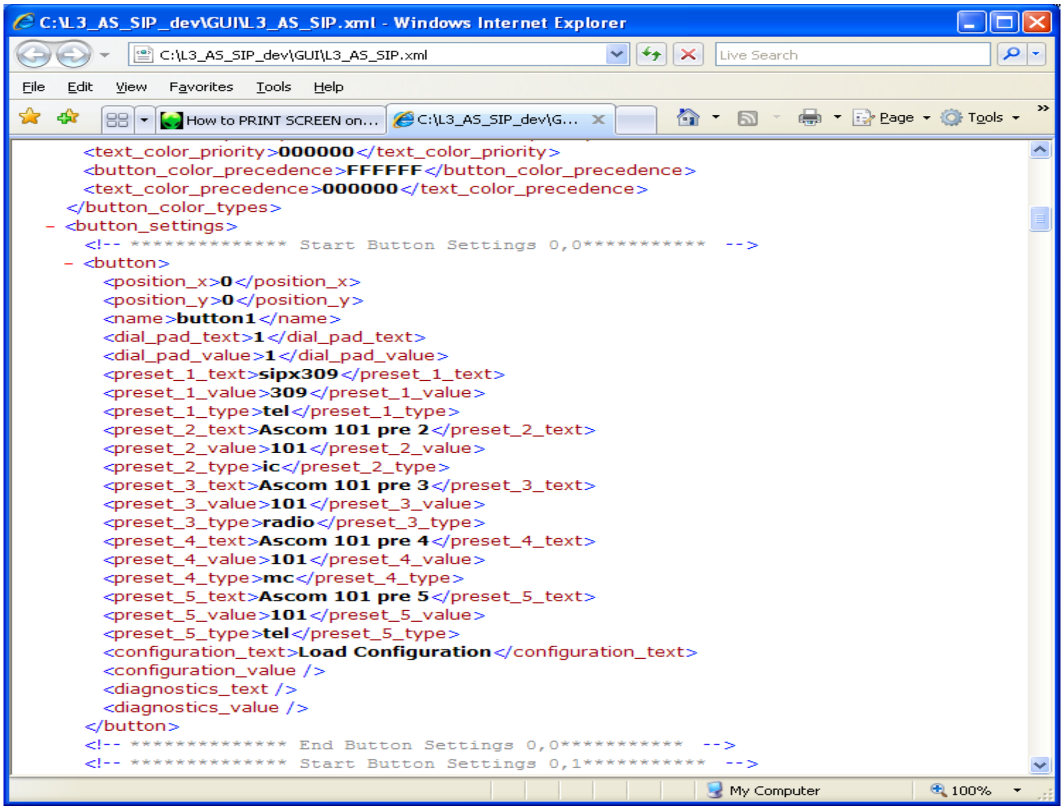
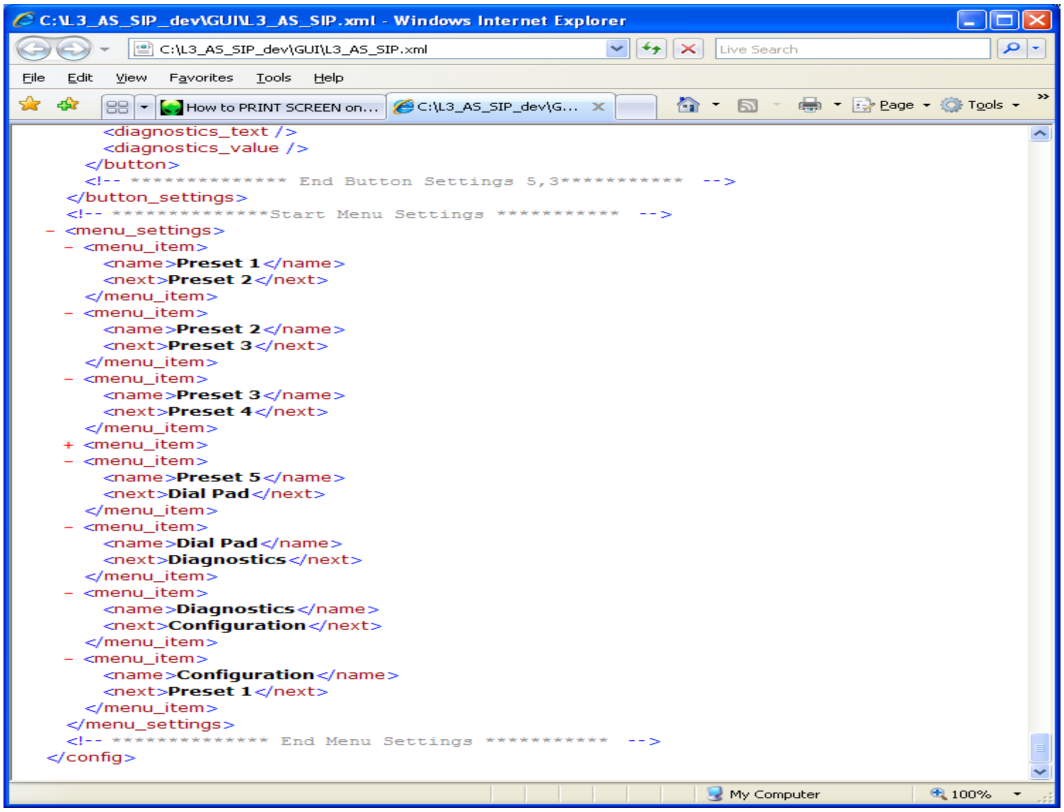


Figure 3-24 L3 AS-SIP Phone Button Configuration XML

3.2.6.2 Menu Settings

Menus are managed via a linked list defined L3_AS_SIP.xml (Figure 3-25). The settings define mode display attributes. Using next and previous tags, menus order can be manipulated – menus removed.



```
<diagnostics_text />
<diagnostics_value />
</button>
<!-- *************** End Button Settings 5,3************ -->
</button_settings>
<!-- ***************Start Menu Settings *********** -->
- <menu_settings>
  - <menu_item>
      <name>Preset 1</name>
      <next>Preset 2</next>
    </menu_item>
  - <menu_item>
      <name>Preset 2</name>
      <next>Preset 3</next>
    </menu_item>
  - <menu_item>
      <name>Preset 3</name>
      <next>Preset 4</next>
    </menu_item>
  + <menu_item>
  - <menu_item>
      <name>Preset 5</name>
      <next>Dial Pad</next>
    </menu_item>
  - <menu_item>
      <name>Dial Pad</name>
      <next>Diagnostics</next>
    </menu_item>
  - <menu_item>
      <name>Diagnostics</name>
      <next>Configuration</next>
    </menu_item>
  - <menu_item>
      <name>Configuration</name>
      <next>Preset 1</next>
    </menu_item>
  </menu_settings>
  <!-- *************** End Menu Settings *********** -->
</config>
```

Figure 3-25 L3 AS-SIP Menus Configuration XML

3.2.7 L3_AS_SIP_Phone Interoperability Tests

Refer to Appendix B for the L3_AS_SIP_Phone interoperability tests performed using the call functions described in paragraph 3.2.3.1 thru paragraph 3.2.3.6.

CHAPTER 4 PHYSICAL NETWORK FEASIBILITY

4.1 Introduction

The objectives of this document are to analyze the concepts and designs covered in the iACT Phase 1 report. The following questions will be evaluated in this chapter.

1) Does the mesh topology (selected in the iACT Phase 1 report) support the requirements for bandwidth and resilience for shipboard use?
2) Can the configuration allow voice traffic to maintain quality of service when the network is loaded with lower priority packets?
3) Can a scheme be created to allow for all packets on a network to have the right priority that can be implemented in the current technologies?
4) Does security degrade the over all performance of the network to make VoIP unusable on board ship?

4.1.1 Scope

It is outside the scope of this document to develop a flawless design, especially in absence of actionable requirements. The purpose of this document is to show a network topology and prove its applicability by analyzing different network aspects important in multi-application traffic scenarios. These scenarios include flow analysis, capacity analysis, performance, load balancing or network reliability, survivability, network security (IPSEC), and Quality of Service (QoS) satisfaction.

The nature of this review is for telephony capabilities, so the evaluation criteria needed to be defined in realm. The use of Mean Opinion Scores (MOS) was used as the main testing method. There were other methods used but the MOS was the final evaluation tool where appropriate.

The network design described in this document is comprehensive in what it covered, but it should be noted that it did not deal with several other important aspects of networking. These are for example, security considerations on designs like threat analysis and threat mitigation by design, setting up demilitarized zones (DMZs), network management (NM) design and impacts, migration of networks including support for legacy capabilities, and IPv4-IPv6 migration, to name a few.

4.1.2 iACT VoIP Network Physical Connectivity

4.1.2.1 Full Mesh

The mesh topology provides the most connectivity by interconnecting the nodes directly. In this case all the edges are meshed, and each edge is only one hop away from each other. This provides better performance, especially for peer-to-peer traffic like Voice

over IP (VoIP) since traffic between edge-switches does not have to pass through the core routers. The trade-offs will be in terms of added links, complexity in configuration when adding nodes, and operations.

4.1.2.2 Partial Mesh

In most network designs, depending on the performance requirements (e.g., maximum number of hops, latency, jitter, network reliability) instead of a full mesh, a partial mesh will suffice. The full network is again a hybrid where the end devices are star-connected to the edges, and the edges are partial meshed based on traffic flow and performance requirements.

4.1.2.3 Dual-Redundant Mesh Network

The two mesh networks operate 100 percent of the time. Data frames are always sent redundantly, and an arbitration algorithm at the destination nodes accepts new arrivals and discards any duplicates. This results in a system that can "fail over" with no switching time. Because of the cost to implement this type of network, it was not considered for this test lab.

4.1.3 iACT Network Topology

4.1.3.1 Overview

Two different topologies are implemented for the network architecture. The objective of Phase 2 of the iACT program is to implement a network design with these two topologies, incorporating the requirements and then analyzing them from the perspective of overall network design. This includes number and types of network nodes, number and types of network links and link bandwidths, fault recovery, performance of real-time applications such as VoIP and Video conferencing, and satisfaction of QoS for different Class of Service (CoS) in normal and stressed condition.

It is noted that although there are multiple categories of applications, the Navy vessel is like a self-contained enterprise location and typical topologies and the principles that apply to enterprise network design apply. Given the size of the user community and the location, the two topologies that constitute the core architecture are distributed-star, and partial mesh. There are other network topologies as detailed in the Phase 1 feasibility study[1] but they are not expected to fit the requirements as well as these two.

Figure 4-1 illustrates the layout of the four core switches and one edge switch used in the iACT test bed. The four core switches are connected in a full mesh configuration while the edge switch is connected in a partial mesh configuration to the core switches.

[1] *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy,* SRN L3COM/HENSCHEL/TR – 2007/001.

All end-user devices are connected to the network through the 48-port edge switch while non-end user devices (i.e. Servers, Controllers, etc.) are connected through one or more of the core switches.

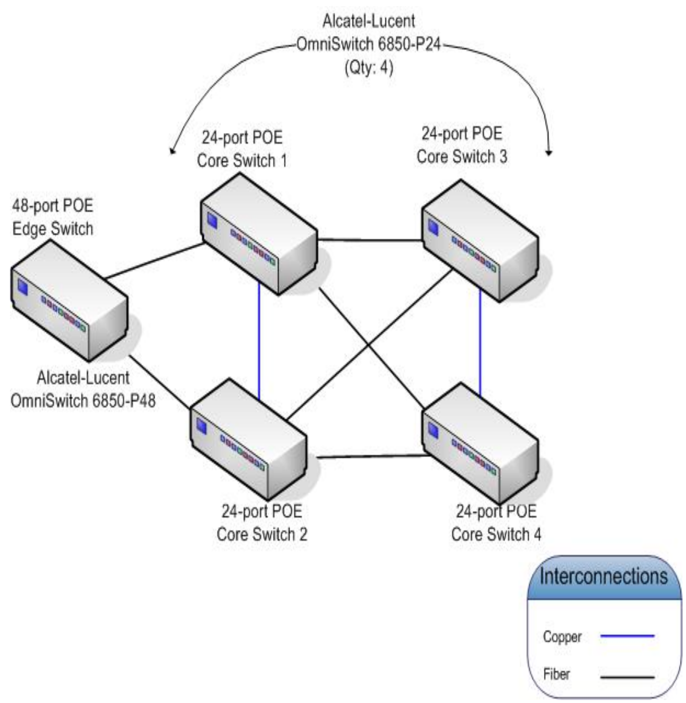


Figure 4-1 Switch Layout

The original layout used Alcatel stacking cables, but these cables resulted in the network having only two core switches. This reduction in switches resulted in L-3 Henschel not being able to test a mesh topology. The final configuration uses both fiber and copper to create the meshed network. The copper replaced the previous stacker cables that were located on the back of the switches.

Figure 4-2 illustrates the layout of the main cabinet. The edge switch is not shown in the illustration since it is mounted to the rear of the cabinet as well as the power supplies for the other Alcatel switches

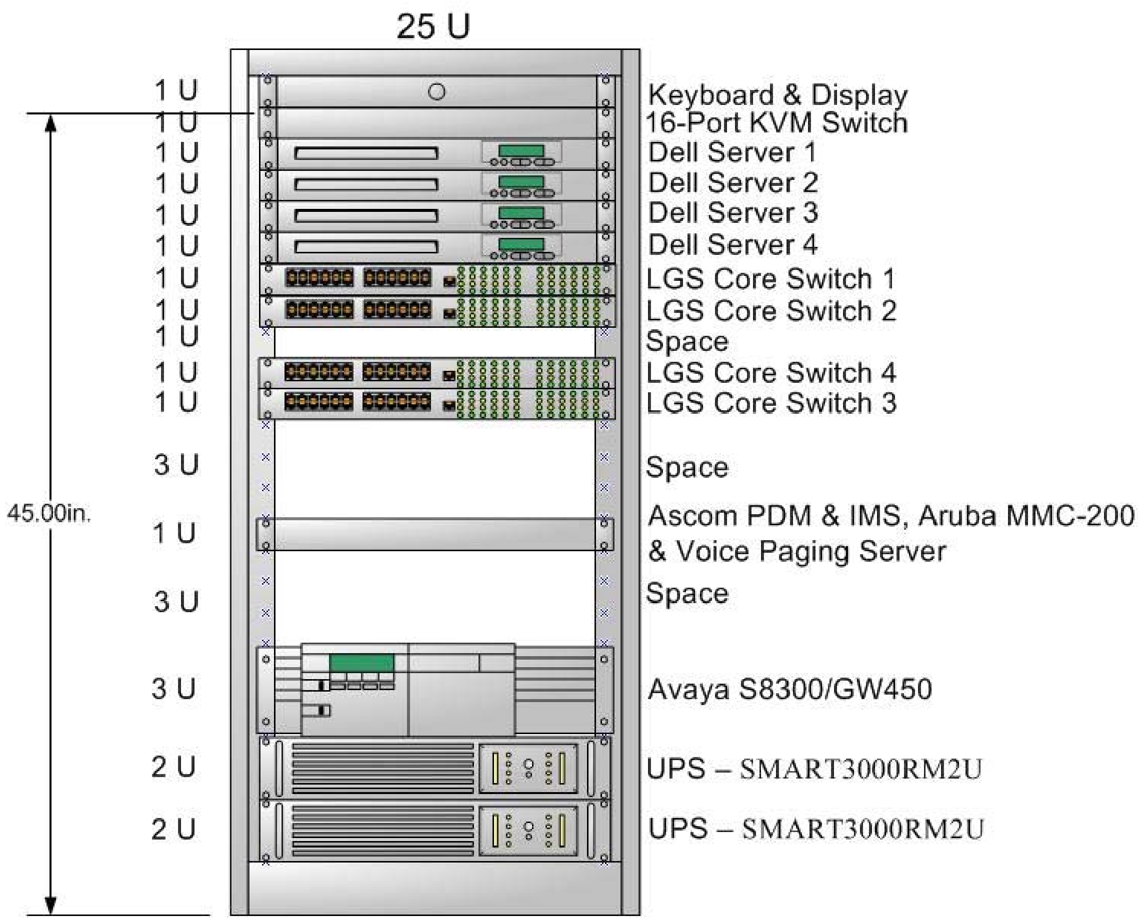


Figure 4-2 Test Bed Layout (Main Cabinet)

4.1.3.2 Gigabit Ethernet Physical Connections

The edge switches are connected to core switches in a partial meshed topology in such a way that the number of hops between edge networks is optimized. The core switch connection is by way of two 1-Gigabit multimode fibers, which provide a high-speed, redundant link to the network backbone (and thus the servers). The core switches are interconnected in a mesh configuration to provide load balancing for increased performance, and also to increase the resiliency of the network in the event that one of the core switches fail.

4.1.3.3 End-User Devices

Table 4-1 lists the end-user devices used for iACT.

Table 4-1 End-User Devices

Device Type	Model
IP Phone	Avaya 4610 SW IP
Wireless Phone	Ascom i75
IP Camera	IQeye 511
Wireless Camera	Axis 211W
IP Speaker	Cyberdata 010844C/020460F
Wireless Access Point	Aruba AP60
PoC	L-3 Henschel IP Communications Terminal
SIP Phone	Polycom SoundPoint IP

4.1.3.4 Servers and Appliances

Table 4-2 lists the servers and appliances used for iACT.

Table 4-2 Servers and Appliances

Device Type	Model
Wireless Infrastructure	Aruba Integrated Message Server
Wireless Infrastructure	Aruba Portable Device Manager
Wireless Infrastructure	Aruba MC-200 Mobility controller
Pager Server	CyberData Page Server
VoIP PBX	Avaya 8300/G450
Dell Servers	R300
Dell Laptops	D630

4.1.4 VLANs for Converged Voice, Video and Data

Figure 4-3 illustrates the layout of the iACT VLANs. A number of VLANs have been created on the switches to reduce the size of the broadcast domain thus reducing the performance impact of broadcasts on the end-devices. The VLANs listed in Table 4-3 are implemented within the iACT switches:

Table 4-3 iACT VLANs

VLAN ID	Purpose	IP Address/Subnet Mask
1	Switch Maintenance	192.168.100.x/24
10	Video	192.168.10.x/24
20	Voice (Land-Line Phone & Announcing System)	192.168.0-3.x/22
40	Navigational Simulation Data	192.168.40.x/24
50	Data (Workstations & Laptop computers)	192.168.50.x/24
70	Wireless (Phones & Wireless Camera)	192.168.70.x/24

The choice for the iACT VLAN design is port-based. In a port-based VLAN, a switch port to an end-device (PC, server, IP phone, speaker, etc.) is associated with a VLAN ID. Traffic from a VLAN switch is tagged with that VLAN ID as it is forwarded through the switched network complying with the IEEE 802.1q standard. This is termed VLAN Tagging (also referred to as *Q-Tagging*). One can associate a VLAN with a specific type of equipment, such as a PC or VoIP phone.

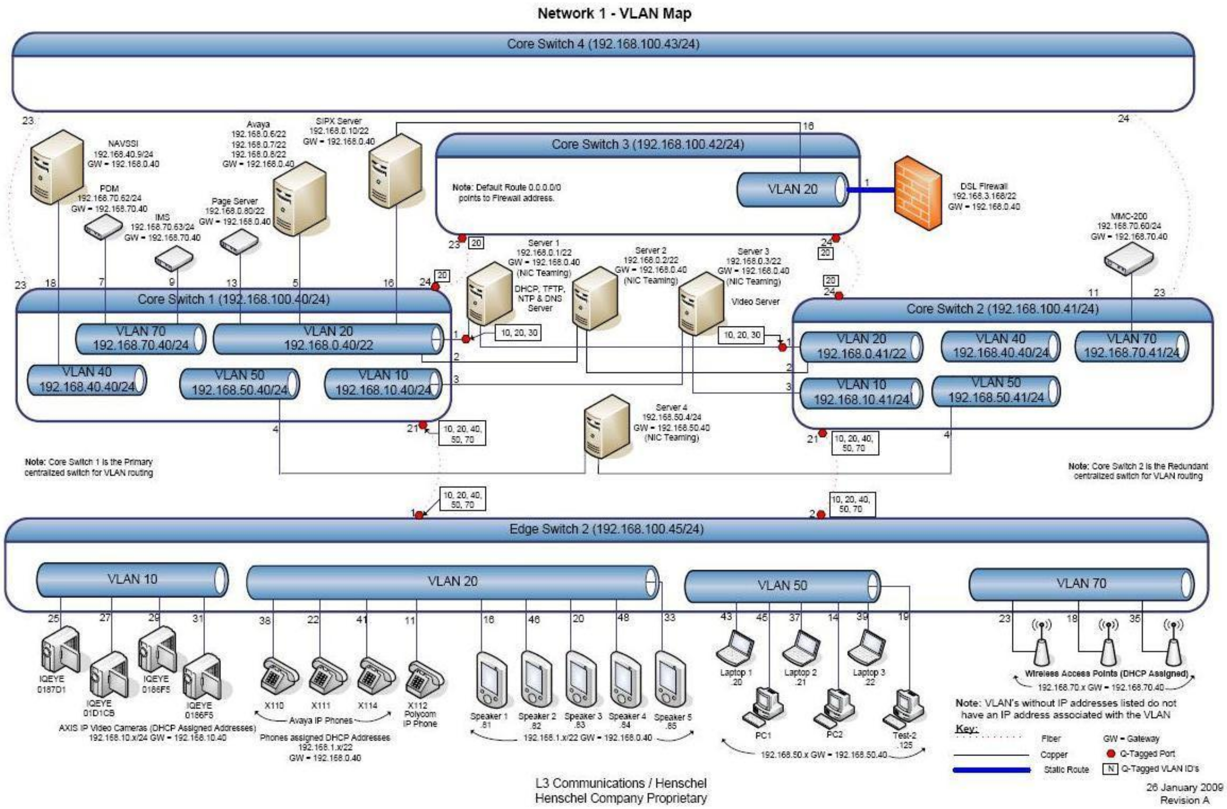


Figure 4-3 iACT VLAN Map

The switches and servers are dual-homed in order to increase survivability through the addition of redundant paths through the network.

4.1.4.1 Spanning Tree Protocol (STP)

The first spanning tree protocol[2] was invented in 1985 at the Digital Equipment Corporation by Radia Perlman.[3]

[2]Spanning Tree Protocol – Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Spanning_tree_protocol, February 3, 2009.

[3]Perlman, Radia (1985), *An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN*, ACM SIGCOMM Computer Communication Review 15 (4): 44–53. doi:10.1145/318951.319004.

In 1990, the IEEE published the first standard for the protocol as 802.1D[4], based on the algorithm designed by Perlman. Subsequent versions were published in 1998[5] and 2004[6], incorporating various extensions.

Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement," declaring which capabilities and options have been implemented[6] to help users determine whether different implementations will interwork correctly.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

4.1.4.2 Rapid Spanning Tree Protocol (RSTP)

In 1998 the IEEE (with document 802.1w) introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP) [2], which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.[7, 8]

RSTP includes the following bridge port roles:

- Root - A forwarding port that has been selected for the spanning-tree topology
- Designated - A forwarding port for every LAN segment

[4] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1990), ANSI/IEEE Std 802.1D, IEEE.

[5] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1998), ANSI/IEEE Std 802.1D, 1998 Edition, Part 3: Media Access Control (MAC) Bridges, IEEE.

[6] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (2004), ANSI/IEEE Std 802.1D - 2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE.

[7] Waldemar Wojdak (March 2003 [CPCI203]), *Rapid Spanning Tree Protocol: A* new solution from an old technology, http://www.compactpci-systems.com/articles/id/?203. Retrieved on 2008-08-04.

[8] *Understanding Rapid Spanning Tree Protocol (802.1w)*, http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml. Retrieved on 2008-11-27.

- Alternate - An alternate path to the root bridge. This path is different than using the root port.
- Backup - A backup/redundant path to a segment where another bridge port already connects.
- Disabled - Not strictly part of STP, a network administrator can manually disable a port.

RSTP is a refinement of STP and therefore shares most of its basic operation characteristics. However there are some notable differences as summarized below:

- Detection of root switch failure is done in 1 hello times, which is 2 seconds if default hello times have not been changed.

- Ports may be configured as edge ports if they are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for Bridge Protocol Data Units (BPDUs) in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.

- Unlike in STP, RSTP will respond to BPDUs sent from the direction of the root bridge. An RSTP bridge will "propose" to its designated ports its spanning tree information. If another RSTP bridge receives this information, determines this is the superior root information, and sets all its other ports to discard. The bridge may send an "agreement" to the first bridge confirming its superior spanning tree information. The first bridge, upon receiving this agreement, knows it can rapidly transition that port to the forwarding state bypassing the traditional listening/learning state transition. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements that allows RSTP to achieve faster convergence times than STP.

As discussed in the port role details above, RSTP maintains backup details regarding the discarding status of ports. This avoids timeouts if the current forwarding ports were to fail or BPDUs were not received on the root port in a certain interval.

4.1.4.3 Multiple Spanning Tree Protocol (MSTP)

The Multiple Spanning Tree Protocol (MSTP)[2], originally defined in IEEE 802.1s and later merged into IEEE 802.1Q-2003, defines an extension to the RSTP protocol to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate spanning tree for each VLAN group and blocks the links that are redundant within each spanning tree.

If there is only one Virtual LAN (VLAN) in the network, single (traditional) STP works appropriately. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the redundant links available by using an alternate spanning tree for different (groups of) VLANs.

4.1.5 Dual-Homing Vital Components

Dual-homing vital components will work with the different network protocols to see if a VoIP device will maintain connection when a single leg of a dual-homed device is lost. It will be evaluated based on whether the configuration allows for the call to be maintained with minimal disruption of the voice path during loss and reconnection of a single leg. End devices are rarely designed with dual-homing in mind. Critical devices for the US Navy will need to be designed with this critical feature included.

4.1.6 Subnetting

Subnetting[9] is used to break the network into smaller more efficient subnets to prevent excessive rates of ethernet packet collision in a large network. Such subnets can be arranged hierarchically, with the organization's network address space partitioned into a tree-like structure. Routers are used to manage traffic and constitute borders between subnets.

A routing prefix is the sequence of leading bits of an IP address that precede the portion of the address used as host identifier. The routing prefix is often expressed as a "subnet mask", which is a bit mask covering the number of bits used in the prefix. It is frequently expressed in quad-dotted decimal representation, e.g., 255.255.255.0 is the subnet mask for the 192.168.1.0 network with a 24-bit routing prefix (192.168.1.0/24).

All hosts within a subnet can be reached in one "hop" (time to live = 1), implying that all hosts in a subnet are connected to the same link.

A typical subnet is a physical network served by one router, for instance an ethernet network (consisting of one or several ethernet segments or local area networks, interconnected by network switches and network bridges) or a Virtual Local Area Network (VLAN). However, subnetting allows the network to be logically divided regardless of the physical layout of a network, since it is possible to divide a physical network into several subnets by configuring different host computers to use different routers.

[9] Subnetwork - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Subnet_Mask, February 3, 2009.

While improving network performance, subnetting increases routing complexity, since each locally connected subnet is typically represented by one row in the routing tables in each connected router. However, with intelligent design of the network, routes to collections of more distant subnets within the branches of a tree-hierarchy can be aggregated by single routes. Existing subnetting functionality in routers made the introduction of Classless Inter-Domain Routing seamless.

4.1.6.1 Single Subnet

Testing was initially performed on a single subnet (no VLANs) to baseline the iACT test bed. In this architecture, all end-devices reside in the same Broadcast Domain. The end result of this is that all end-devices must spend time to process every broadcast which appears on the network thus impacting end-device performance across the entire network.

4.1.6.2 Multiple Subnets

VLAN's are added to the design to reduce the size of the Broadcast Domain. Broadcasts are limited to the VLAN they originate on.

4.1.7 Routing Protocols

4.1.7.1 Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) [10] is a dynamic routing protocol used in local and wide area networks. It is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). The original version is now known as RIP. Both versions are still in use today, however, they are considered technically obsolete by more advanced techniques, such as Open Shortest Path First (OSPF) and the OSI protocol IS-IS. Since the advent of IPv6, the next generation of the Internet Protocol RIP has been adapted, known as RIPng (RFC 2080, 1997), for use with IPv6.

4.1.7.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) [11] is a dynamic routing protocol for use in Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol and falls into the group of interior gateway protocols, operating within an autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4[12].

---

[10] Routing Information Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Routing_Information_Protocol, February 3, 2009.

[11] Open Shortest Path First - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/OSPF, February 3, 2009.

[12] Moy, J. (April 1998). *OSPF Version 2*. Internet Engineering Task Force. Retrieved on 2007-09-28.

The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008)[13]. OSPF is perhaps the most widely-used interior gateway protocol (IGP) in large enterprise networks; IS-IS, another link-state routing protocol, is more common in large service provider networks. The most widely-used exterior gateway protocol (EGP) is BGP.

4.1.7.3 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) [14] is the core routing protocol of the internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rule sets.

BGP was created to replace the EGP routing protocol to allow fully decentralized routing in order to allow the removal of the National Science Foundation Network (NSFNet) internet backbone network. This allowed the internet to become a truly decentralized system. Since 1994, version 4 of the protocol has been in use on the internet. All previous versions are now obsolete. The major enhancement in Version 4 was support of Classless Inter-Domain Routing and use of route aggregation to decrease the size of routing tables. Since January 2006, version 4 is codified in RFC 4271, which went through well over 20 drafts based on the earlier RFC 1771 Version 4. The RFC 4271 version corrected a number of errors, clarified ambiguities, and also brought the RFC much closer to industry practices.

Most internet users do not use BGP directly. However, since most Internet Service providers must use BGP to establish routing between one another (especially if they are multi-homed), it is one of the most important protocols of the internet. Compare this with Signaling System 7 (SS7), which is the inter-provider core call setup protocol on the PSTN. Very large private IP networks use BGP internally, however. An example would be the joining of a number of large Open Shortest Path First (OSPF) networks where OSPF by itself would not scale to size. Another reason to use BGP is multi-homing a network for better redundancy either to a multiple access points of a single ISP (RFC 1998) or to multiple ISPs.

4.1.8 Quality of Service

4.1.8.1 Overview

Quality of Service (QoS) is a collective measure of the level of service delivered to the customer. QoS is considered the level of assurance for a particular application that the network can meet its service requirements.

---

[13] Coltun, R.; D. Ferguson, J Moy, A. Lindem (July 2008). *OSPF for IPv6*. Internet Engineering Task Force. Retrieved on 2008-07-23.

[14] Border Gateway Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/BGP, February 3, 2009.

From a technical perspective, QoS can be characterized by several performance criteria, such as availability (low downtime), throughput, connection setup time, percentage of successful transmissions, speed of fault detection and correction, etc. In an IP network, QoS can be measured in terms of bandwidth, packet loss, delay, and jitter. In order to provide a high QoS, the IP network needs to provide assurances that for a given session or set of sessions, the measurement of these characteristics will fall within certain bounds[2]. This is critical for VoIP since it uses User Datagram Protocol (UDP) that is a connectionless protocol that makes no guarantee that the data will get to its destination. UDP is used because of the performance gains over Transmission Control Protocol (TCP) that ensures that all data arrives accurately and one-hundred percent intact.

4.1.8.2 Mean Opinion Score/Perceptual Evaluation of Speech Quality

Modern communications networks include elements (bad coding, error-prone channels and voice activity detection) that cannot reliably be assessed by conventional engineering metrics as signal-to-noise ratio. One way to measure customer perception of the quality of these systems is to conduct a subjective test involving panels of human subjects. However, these tests are expensive and unsuitable for such applications as real-time monitoring.

Perceptual Evaluation of Speech Quality (PESQ) provides an objective measure that predicts the results of subjective listening tests on telephony systems. To measure speech quality, PESQ uses a sensory model to compare the original, unprocessed signal with the degraded version at the output of the communications system.

The result of comparing the reference and degraded signals is a quality score. This score is analogous to the subjective Mean Opinion Score (MOS) measured using panel tests according to ITU-T P.800.

PESQ incorporates many new developments that can distinguish it from earlier models for assessing codecs. These innovations allow PESQ to be used with confidence to assess end-to-end speech quality as well as the effect of such individual elements as codecs[15].

The MOS value is an indication of the quality of voice information on a scale of 1 to 5 with 5 being perfect and 1 being inaudible. It is a close approximation of the average rating that would be assigned to voice if it were to be evaluated by human listeners (typically 16 or more). Due to human idiosyncrasies (in general people tend not to assign the highest rating to things) and also that no voice reproduction equipment is perfect, the maximum MOS rating tends to be closer to 4.5.

---

[15] *Voice Quality Testing Reference* Document (PSQM, PAMS, PESQ LQ/LQO/WB), GL Communications Inc., June 2008.

4.1.8.3 Latency, Jitter, and Packet Loss

4.1.8.3.1 Latency

Latency generally refers to the physical distance that a phone call must travel to reach a service provider. When you make a phone call with VoIP, the sounds you make are cut into thousands of little pieces, called packets, and then sent through the internet to your service provider. These packets travel so fast that the process of traveling and reassembling them to the phone at the other end of the conversation generally takes milliseconds.

Usually, most US residents are not affected by latency with their VoIP providers. If the roundtrip travel time of the packet takes more then 250 milliseconds the quality of the communication may experience some issues due to latency. Most commonly, this occurs when trying to connect to a US service provider from an international location. Latency can occur in both VoIP and traditional phone systems.

Many VoIP providers have established multiple hosts to reduce Latency and provide a quick connection from any location. One of the benefits of using VoIP over traditional phone systems is that internet speed is constantly increasing, helping to keep Latency down. Additionally, many VoIP companies provide service centers located in specific areas to ensure Latency is low, regardless of your location[16].

4.1.8.3.2 Jitter

Although average LAN utilization is typically quite small, congestion does often occur during short periods. Worst case delay variation is bounded by the maximum back-off time used in the Ethernet contention algorithm and in some systems is also bounded by the inter-packet delay. If the VoIP end system has been unable to get access to the LAN by the maximum back-off time or by the time the next packet is scheduled for transmission, then it may discard the packet. In the case of 100 Mbit Ethernet the maximum back-off time is in the millisecond range and hence should not be a major source of jitter. LAN congestion typically results in a spiky delay waveform as one packet may be delayed; however, the following packet may get access to the LAN immediately.

When packets are received with a timing variation from when they were sent, a quality issue of jitter may be noticed. When jitter occurs, participants on the call will notice a delay in phone conversation. You may have experienced this with your traditional phone service from time to time. Many VoIP providers reduce or eliminate jitter by controlling jitter and time issues within their networking equipment[16].

---

[16] DeLorenzo, Alfredo, May 23, 2006, www.voip.com, *Voice Quality of Service*.

It is also managed by jitter buffers built into the VoIP phone devices to smooth out the packets. It is many times coupled with a packet loss concealment logarithm that replays packets as required to conceal the missing sections of speech that was in the delayer or lost packets.

4.1.8.3.3 Packet Loss

In VoIP systems, packet loss can take place when a large amount of network traffic hits the same internet connection. When talking on a VoIP system, packet loss can be identified with an echo or tin-like sound. Packet loss is most commonly measured in percentages. For VoIP use, packet loss should not exceed 1%. A one percent packet loss will result in a skip or clipping approximately once every three minutes.
VoIP customers can help to reduce packet loss by reducing high-traffic tasks (such as uploading files or sending emails with large attachments) while on the telephone[16].

4.1.9 Priority Queuing

4.1.9.1 Ethernet Packet Header Priority

The IEEE 802.1p (and IEEE 802.1Q) standard specifies an extra field for the Ethernet MAC header. This field is called the Tag Control Info (TCI) field, and is inserted between the source MAC address and the MAC Type/Length field of an ethernet packet (Figure 4-4 and Figure 4-5) [17]. This field contains a 3-bit priority field that is used for priority handling. Thus, the standard defines 8 different levels of priority. However, most Ethernet switches available today that support priority queuing have only 2 or 4 queues. Note that the OmniSwitch 6850 used for iACT has eight priority queues.

A switch with two priority queues will put ethernet packets with priority tags set to 4 or higher in the high priority queue while all other packets will be put in the low priority queue. Both unmanaged and managed switches can support this feature. Thus, no switch configuration is needed. A disadvantage with this method is that most stations up to now do not support priority tagging. Configuring the switch to remove the tags after switching can solve this, and before the packets are sent on the output ports where stations without support for this feature are connected. This requires managed switch operation.

Another potential problem is the existence of other ethernet switches in the network that do not support priority tagging - i.e. the maximum packet size will, due to the tag, increase by 4 bytes to 1522 bytes, and some switches will not forward packets with a packet length larger than 1518 bytes.

[17] The Industrial Ethernet Book, *VoIP Drives Real Time Ethernet*, Issue 5:29.

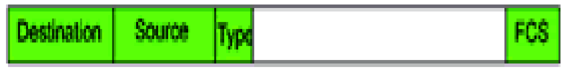


Figure 4-4 MAC Header (Layer 2)

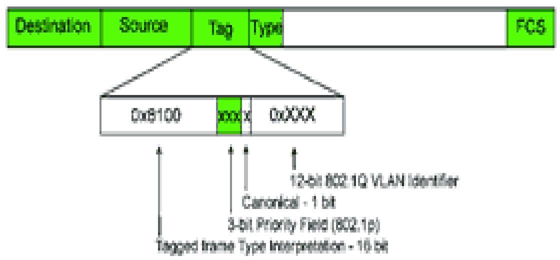


Figure 4-5 MAC Header Layer with Tag

4.1.9.2 IP Header DiffServ

Differentiated Services (Diffserv) [18] prioritizes certain types of traffic like voice traffic over other types of communications. It works by categorizing IP packets into classes. The 6 bits in the type-of-service byte contained in the IP header of each packet, specifies a particular behavior type which determines the packet-forwarding scheme and priority. Differentiated services can offer the following:

- Expedited Forwarding (EF), which defines minimum delay and jitter. Preferred mode for the VoIP, etc.
- Assured Forwarding (AF), which introduces three selectable packet drop rates. During congestion, packets with a high drop precedence are discarded.
- Best effort picks up the remains of the bandwidth.

DiffServ can be used as a QoS mechanism in enterprise networks. It is scalable. DiffServ marking at the edge is read and understood at the core and the packets are forwarded based on the above mentioned priority schemes. Such QoS services are not part of any negotiation or signaling between devices themselves and rules are assigned by local network administrators. These assigned tags are passed in the packet and are not subject to change during the process of auto-negotiation or other forms of signaling. Such an approach is called Soft QoS. 802.1p, IP Precedence and DiffServ are the examples of soft QoS techniques.

---

[18] The Industrial Ethernet Book, *Quality of Service for High Priority Networks*, Issue 41:36.

4.1.9.3 Real-time Transport Protocol

Real-time Transport Protocol (RTP) uses UDP for transport over IP. This means it uses a connectionless method of communication, which works well for getting as much data transmitted to the destination as soon as possible. The fact that it does not offer any guarantee of delivery is its major drawback.

RTP defines a standardized packet format for delivering audio and video over the internet. It was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889, and superseded by RFC 3550 in 2003.

RTP is frequently used in streaming media systems (together with the Real-time Streaming Protocol (RTSP)) as well as in video-conferencing and push-to-talk systems. For these it carries media streams controlled by H.323 or Session Initiation Protocol (SIP) signaling protocols, making it the technical foundation of the VoIP industry.

RTP is usually used in conjunction with the Real-time Transport Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video) or out-of-band signaling (DTMF), RTCP is used to monitor transmission statistics and quality-of-service QoS information. When used in conjunction, RTP is usually originated and received on even port numbers, whereas RTCP uses the next higher odd port number.

4.1.10 Network Address Translation

4.1.10.1 Impact of NAT on SIP and RTP Session Border Controller

There are several 'points of impact' where SIP finds Network Address Translation (NAT) problematic, and it is not limited to NAT. RTP also has problems with NAT. Because SIP packets go out from an NAT client with their private (and unroutable) IP addresses coded into the message headers and SDP bodies, they are not processed by a NAT device that operates only on the IP packets as they pass by. This means that when the packets get to their destination, they are processed and responded to using completely useless source address information.

There are three major problems of NAT in SIP and RTP:

1. The VIA header problem: Responses to requests cannot be routed back to the originating party, as the supplied addressing information is not globally routable.

2. The CONTACT header problem: This refers to the fact that future requests would be routed incorrectly, again due to non-routable addresses being supplied.

3. The RTP problem: The final problem in the NAT/SIP category is in connection with RTP (the voice part of the session). The SDP messages which are used to negotiate the session format (codecs, ports, IP's etc), which are often enclosed within the SIP message body, and thus not processed by a SIP proxy according to IETF standards,

will contain non-routable contact information as well (i.e. the internal address, such as 192.168.x.x). This is a difficult problem to solve.

There are several solutions to allow SIP to traverse NAT effectively. None of them are ideal, and much of it is external to SIP. The following paragraphs discuss the techniques applied within the protocol, and common third party solutions to the resolution of these problems.

1. The VIA header answer: This is solved within SIP. When a message arrives at a SIP server or UA, a comparison is made between the address the packet came from, and the one that is listed in the VIA header. If there is a difference, then the correct IP address (the one from which the packet originated from) is written as a parameter 'received=', and is added to the VIA header.

2. The CONTACT header answer: This is a similar problem to the VIA header issue, and is solved in the same way, updating the CONTACT header instead. The CONTACT header is referred to for communications that occur some time after an original request (such as BYE's or re-INVITE's), and this can cause additional problems, for the following reason. NAT bindings are kept active on the NAT device for only a finite amount of time if SIP is being transported over UDP. Solutions to this include using TCP for SIP instead of UDP (which is a connection-oriented protocol and so bindings and associated timeouts are not a problem), employing some kind of keep_alive program to maintain NAT bindings, or using STUN/TURN servers, or even a Back-to-Back User Agent (B2BUA).

4.1.10.2 The RTP answer

For instances where only one UA is behind a NAT device, symmetric NAT can be used. This effectively synchronizes the two RTP streams; the recipient of the successful RTP stream (i.e. the globally routable UA in the session) transmits its RTP stream using the source IP of that RTP flow, ignoring the one that SDP has told it to use.

For instances where both users are behind NAT, you can employ a RTP proxy/media server/B2BUA of some kind to relay voice, breaking the call into two separate legs or you can use the Traversal Using Relay NAT (TURN) protocol.

4.1.11 Security

4.1.11.1 IPSEC Delays Session/Call Establishment

Most IPsec implementations consist of an IKE daemon that runs in user space and an IPsec stack in the kernel that processes the actual IP packets.

User-space daemons have easy access to mass storage containing configuration information, such as the IPsec endpoint addresses, keys and certificates, as required. Kernel modules, on the other hand, can process packets efficiently and with minimum overhead—which is important for performance reasons.

The IKE protocol uses UDP packets, usually on port 500, and generally requires 4-6 packets with 2-3 turn-around times to create an SA on both sides. The negotiated key material is then given to the IPsec stack. For instance, this could be an AES key, information identifying the IP endpoints and ports that are to be protected, as well as what type of IPsec tunnel has been created. The IPsec stack, in turn, intercepts the relevant IP packets if and where appropriate and performs encryption/decryption as required. Implementations vary on how the interception of the packets is done - for example, some use virtual devices; others take a slice out of the firewall, etc.

4.1.11.2 Transport Layer Security (TLS)

The Transport Layer Security (TLS) [19] protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the internet using cryptography.

In typical end-user/browser usage, TLS authentication is *unilateral*: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous). More strictly speaking, *server authentication* means different things to the browser and to the end-user. At the browser level, it only means that the browser has validated the server's certificate — i.e., checked the digital signatures of the server certificate's issuing CA-chain (chain of Certification Authorities that guarantee bindings of identification information to public keys — see public key infrastructure). Once validated, the browser is justified in displaying a security icon (such as "closed padlock"). But mere validation does NOT "identify" the server to the end-user. For true identification, it is incumbent on the end-user to be diligent in scrutinizing the identification information contained in the server's certificate (and indeed its whole issuing CA-chain). This is the only way for the end-user to know the "identity" of the server. In particular: the "locked padlock" icon has no relationship to the URL, DNS name or IP address of the server. This is a common misconception. Such a binding can only be securely established if the URL name or address is specified in the server's certificate itself. Understanding this subtlety makes it very difficult for end-users to properly assess the security of web browsing (though this is not a shortcoming of the TLS protocol itself - it's a shortcoming of PKI).

[19] Transport Layer Security - Wikipedia, the free encyclopedia, Transport Layer Security - Wikipedia, the free encyclopedia, January 30, 2009.

This is known as mutual authentication. Mutual authentication requires that the TLS client-side also hold a certificate (which is not usually the case in the end-user/browser scenario). Unless, that is, TLS-PSK or the Secure Remote Password (SRP) protocol or some other protocol is used that can provide strong mutual authentication in the absence of certificates.

TLS involves three basic phases:

1. Peer negotiation for algorithm support
2. Key exchange and authentication
3. Symmetric cipher encryption and message authentication

During the first phase, the client and server negotiate *cipher suites*, which determine the ciphers to be used, the key exchange and authentication algorithms, as well as the message authentication codes (MACs). The key exchange and authentication algorithms are typically public key algorithms, or as in TLS-PSK preshared keys could be used. The message authentication codes are made up from cryptographic hash functions using the HMAC construction for TLS, and a non-standard pseudorandom function for SSL.

Typical algorithms are:

1. For key exchange: RSA, Diffie-Hellman, ECDH, SRP, PSK
2. For authentication: RSA, DSA, ECDSA
3. Symmetric ciphers: RC4, Triple DES, AES, IDEA, DES, or Camellia. In older versions of SSL, RC2 was also used.
4. For cryptographic hash function: HMAC-MD5 or HMAC-SHA are used for TLS, MD5 and SHA for SSL, while older versions of SSL also used MD2 and MD4.

4.1.11.3 Secure Sockets Layer (SSL)

Secure Sockets Layer [20], a protocol developed by Netscape for transmitting private documents via the internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http*:

4.1.12 IP Multicasting

IP Multicasting is a technique for single to multiple communications over an IP infrastructure. It scales to a larger receiver population by not requiring prior knowledge of whom or how many receivers there are.

[20] Webopedia, SSL definition, http://www.webopedia.com/TERM/S/SSL.html

Multicast utilizes network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers only where necessary.

Key concepts in IP Multicast include an IP Multicast group address, a multicast distribution tree and receiver driven tree creation.

An IP Multicast group address is used by sources and the receivers to send and receive content. Sources use the group address as the IP destination address in their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group. For example, if some content is associated with group 239.1.1.1, the source will send data packets destined to 239.1.1.1. Receivers for that content will inform the network that they are interested in receiving data packets sent to the group 239.1.1.1. The receiver "joins" 239.1.1.1. The protocol used by receivers to join a group is called the Internet Group Management Protocol (IGMP).

Once the receivers join a particular IP Multicast group, a multicast distribution tree is constructed for that group. The protocol most widely used for this is Protocol Independent Multicast (PIM). It sets up multicast distribution trees such that data packets from senders to a multicast group reach all receivers which have "joined" the group, e.g. all data packets sent to the group 239.1.1.1 are received by receivers who joined 239.1.1.1.

IP Multicast does not require a source sending to a given group to know about the receivers of the group. The multicast tree construction is initiated by network nodes which are close to the receivers or is receiver driven. This allows it to scale to a large receiver population.

It is unlikely that any single router in the internet maintains state for all multicast trees. This is a common misunderstanding compared to unicast. A unicast router needs to know how to reach all other unicast addresses in the internet, even if it does this using just a default route. For this reason, aggregation is key to scaling unicast routing. Also, there are core routers that carry routes in the hundreds of thousands because they contain the internet routing table. On the other hand, a multicast router does *not* need to know how to reach all other multicast trees in the internet. It only needs to know about multicast trees for which it has receivers downstream of it. This is key to scaling multicast. It is very unlikely that core internet routers would need to keep state for all multicast distribution trees; they only need state for trees with downstream membership. When this type of router joins a shared forwarding tree it is referred to as *graft* and when it is removed it is called a *prune*.

4.1.13 Test Results

4.1.13.1 Voice Quality Test Description Test Files

Four files containing speech (2 Male and 2 Female) are transmitted through the network-under-test. Because different people's speech may be distorted in different ways, it is usual to pass speech from four different talkers – 2 adult male, 2 adult female – through each condition[15]. Speech consists of a certain number of sounds that are capable of being phonemically grouped. Each phoneme is subject to a wide speaker dependent variation and will be affected by its association with other phonemes and the context in which it is produced[21].

4.1.13.2 Test Conditions

Testing was performed using the following conditions with each test condition being built from the previous one:

1. No VLANs, QoS, or Security implemented (Baseline) (Test Condition 1)
2. Test condition 1 + VLANs implemented (Test Condition 2)
3. Test condition 2 + QoS implemented (Test Condition 3)
4. Test condition 3 + Data file transfers (Test Condition 4)

For each test condition listed above, MOS scores (PESQ), Average Jitter, and RTD values are collected. All tests are run for a minimum of 1/2 hour. The tests consisted of the following:

1. Sending voice files between phones without any other network activity excluding basic network overhead such as ARP requests and replies.
2. Sending voice files between phones with video data activity from the four IP cameras and one wireless camera occurring simultaneously.
3. Sending voice files between phones with video data and navigational data (from NAVSSI simulator) occurring simultaneously.
4. Sending voice files between phones with video data, navigational data (from NAVSSI simulator), and multiple gigabyte file transfers between PC's occurring simultaneously.

Four voice files are used for the testing (Female1, Female2, Male1, and Male2). In all cases, the PESQ value and Average Jitter are shown in two charts, one for a Female voice and one for a Male voice. The left side of each chart is the first utterance (i.e. Female1 or Male1) and the right side is the second utterance (i.e. Female2 or Male2).

---

[21] *Understanding Voice Files*, GL Communications Inc.

4.1.13.3 Voice Quality Test Setup

Figure 4-6 shows the test setup used to measure MOS (Mean Opinion Score) and RTD (Round Trip Delay) of the iACT network. The first step in testing is to establish a call between the two IP phones. Once the call is established and the hand-set of both phones are "off-hook" the phones are connected to the Phone Input of their respective UTA (Universal Telephone Adapter). A script is started on Laptop 3 which sends the voice files to Laptop 2.

Laptop 1 copies the voice files from Laptops 2 and 3 and compares the "Reference" files (files sent) to the "Degraded" files (files received) using GL Communications VQT application software in order to determine the MOS score and jitter of the attached network.

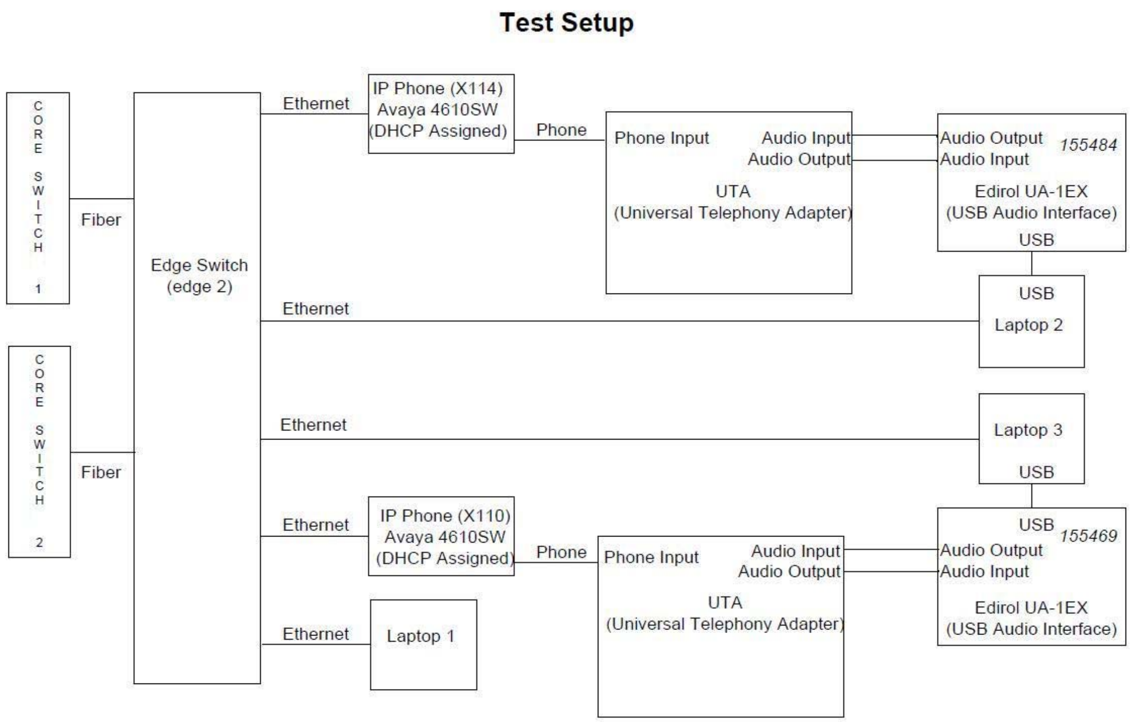


Figure 4-6 iACT Voice Quality Test Setup

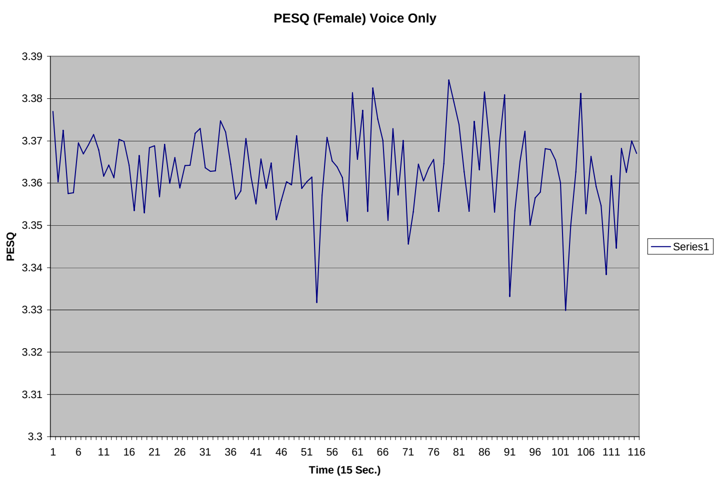
4.1.13.4 Test Condition 1 (Baseline)

The baseline tests were run on a single subnet (no VLANs). Also, QoS was not enabled on the switches. It consisted of three scenarios as follows:

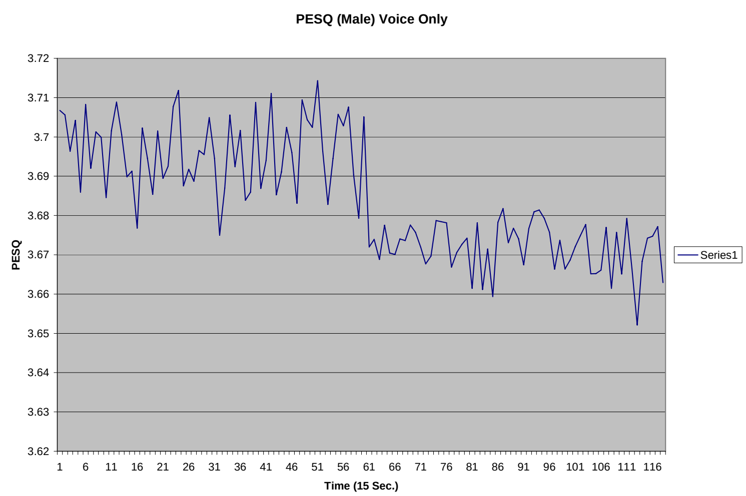
1. Voice only – Voice files sent between IP Phones without any other network activity other then overhead such as ARP Requests and Replies.
2. Voice and Navigational Data – Navigational data multicast from Server #1 on Core switch 1 and received by the NAVSSI receiver running on a PC connected to edge switch 2. NAVSSI was setup to transmit two 50Hz data streams, one Aft and one forward.
3. Voice, Navigational, and Video data – With scenario 2 running, video data was streamed from the four IP cameras to server #3.
4. Voice, Navigational, Video, and File transfer data – With scenario 3 running, ~10GB of data was copied from Laptop #3 to Server #1.

4.1.13.4.1 MOS/PESQ

Figures 4-7 thru Figure 4-10 shows PESQ scores.



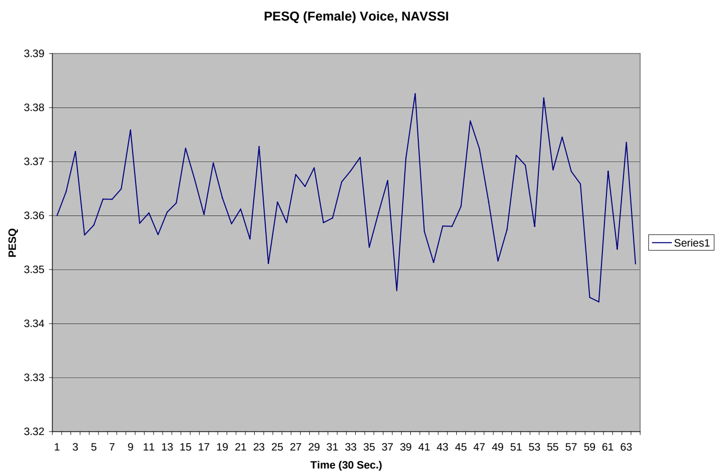
Average PESQ = 3.36



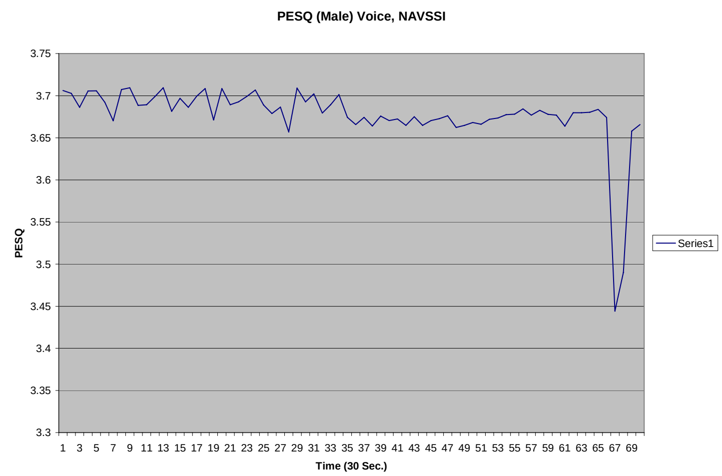
Average PESQ = 3.68

Figure 4-7 PESQ Score (Voice Only)

Note: There is a drop in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.



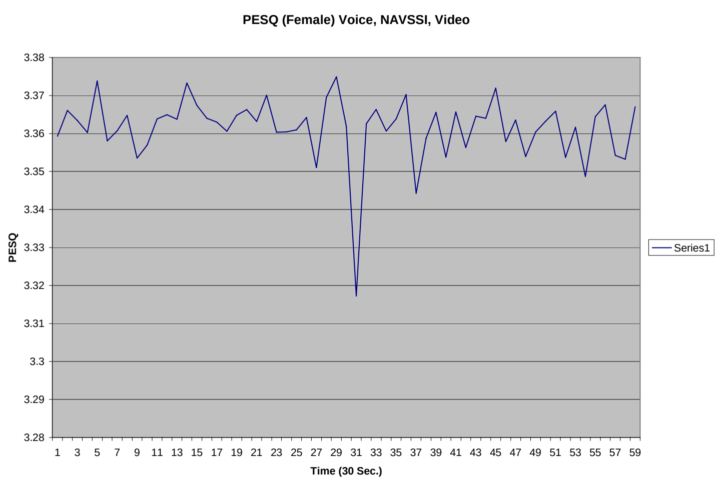
Average PESQ = 3.36



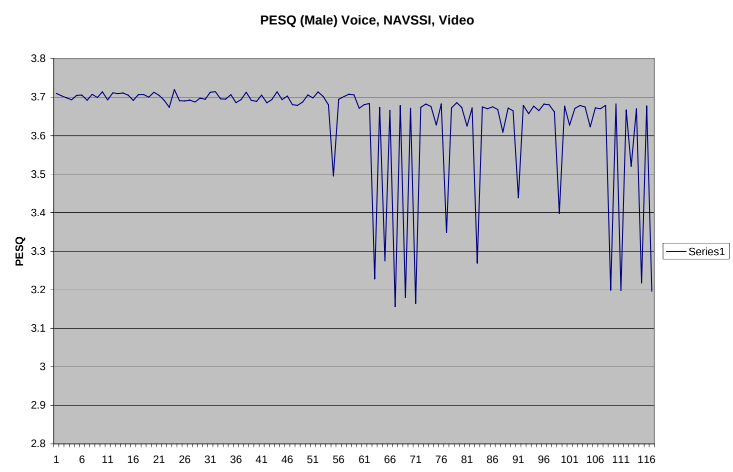
Average PESQ = 3.67

Figure 4-8 PESQ Score (Voice and Navigational Data)

Note: There is a drop in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.



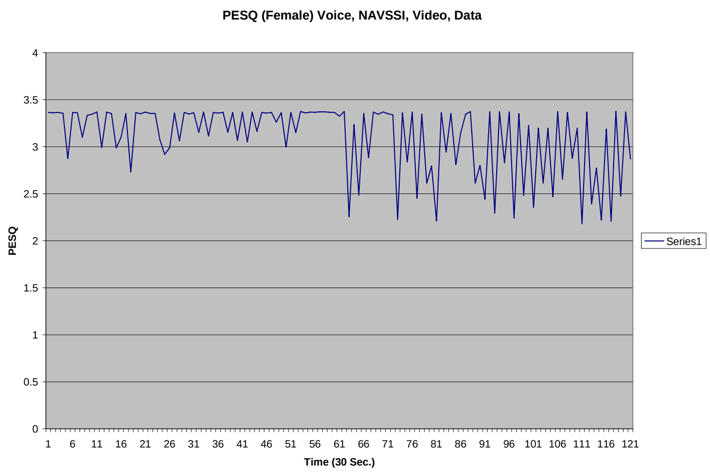
Average = 3.34



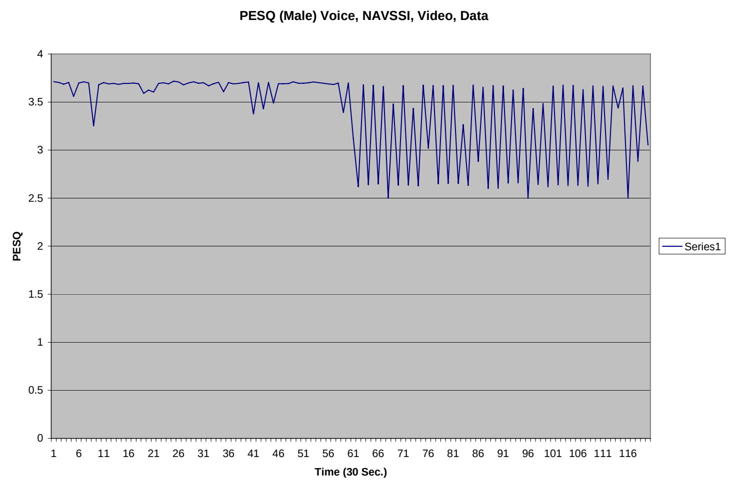
Average = 3.63

Figure 4-9 PESQ Score (Voice, Navigational, and Video Data)

Note: There is a drop in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.



Average = 3.1



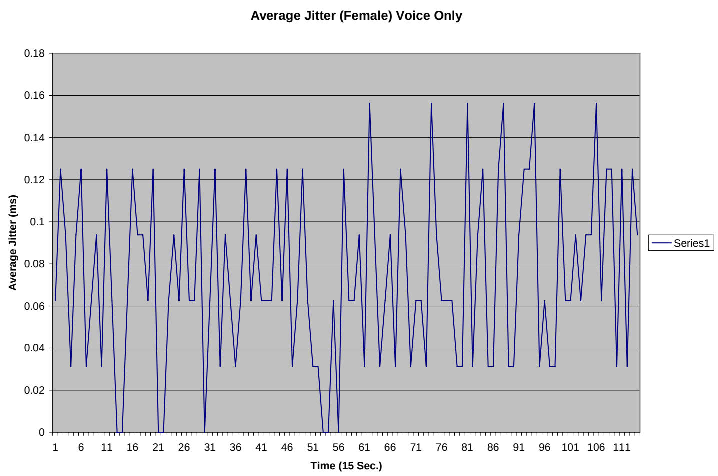
Average = 3.4

Figure 4-10 PESQ Score (Voice, Navigational, Video Data, and File Transfer Data)

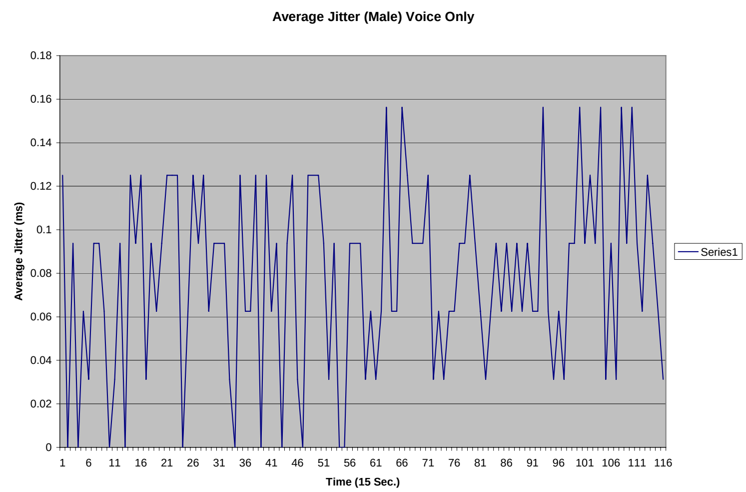
Note: There is a change in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.

4.1.13.4.2 Average Jitter

Figure 4-11 thru Figure 4-14 show the average jitter (Figure 4-11 shows jitter for voice-only communications).

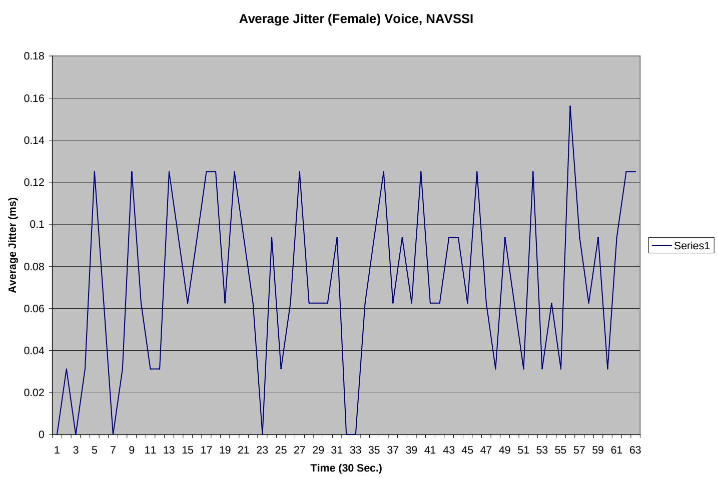


Average = .074 ms

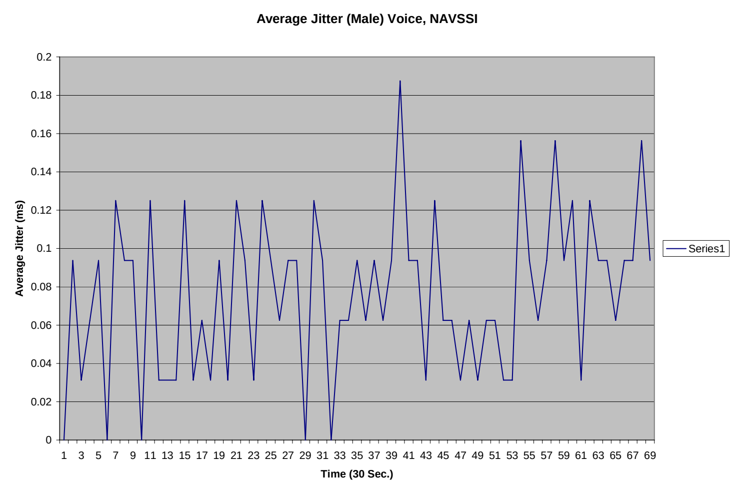


Average = .078 ms

Figure 4-11 Average Jitter (Voice Only)

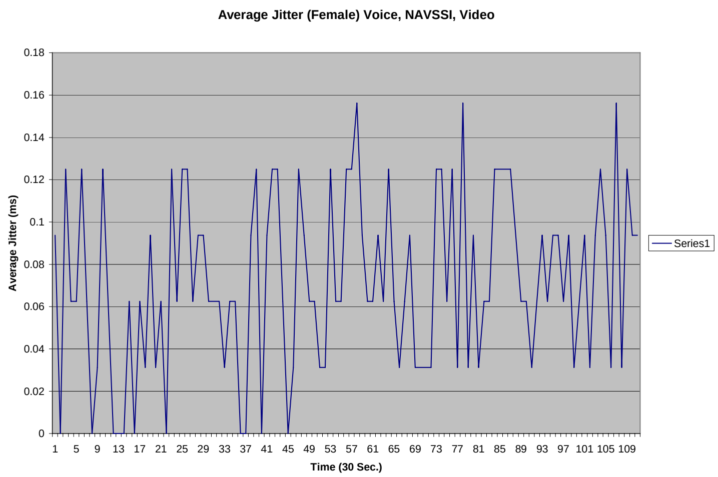


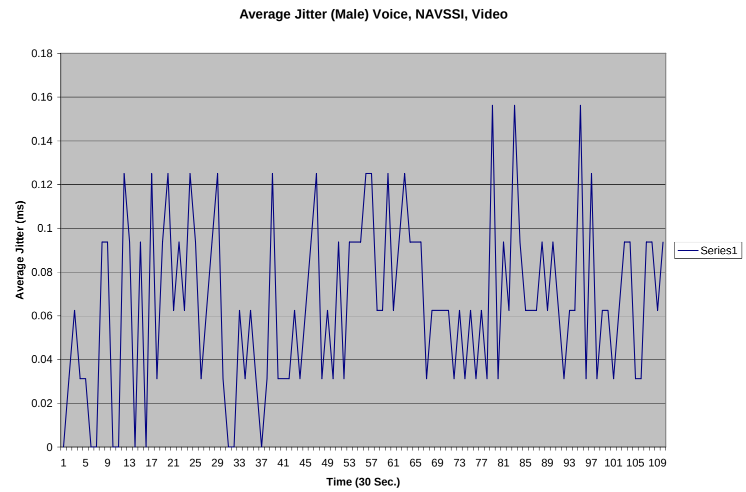
Average = .072 ms



Average = .076 ms

Figure 4-12 Average Jitter (Voice and Navigational Data)

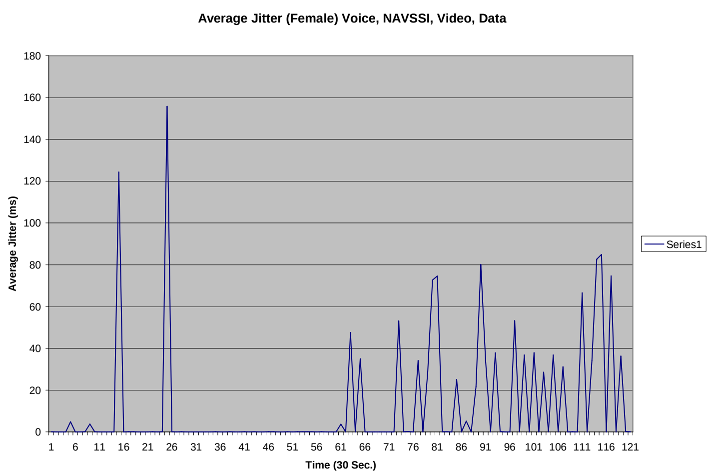


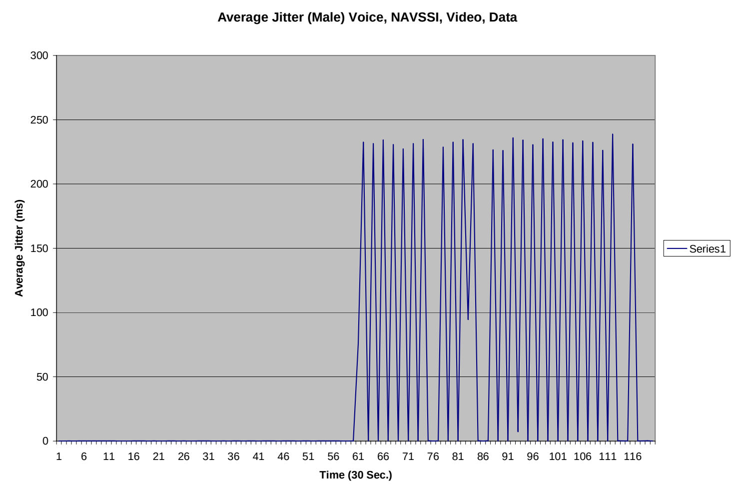


Average = .072 ms

Average = .065 ms

Figure 4-13 Average Jitter (Voice, Navigational, and Video Data)





Average = 12.0

Average = 49.8

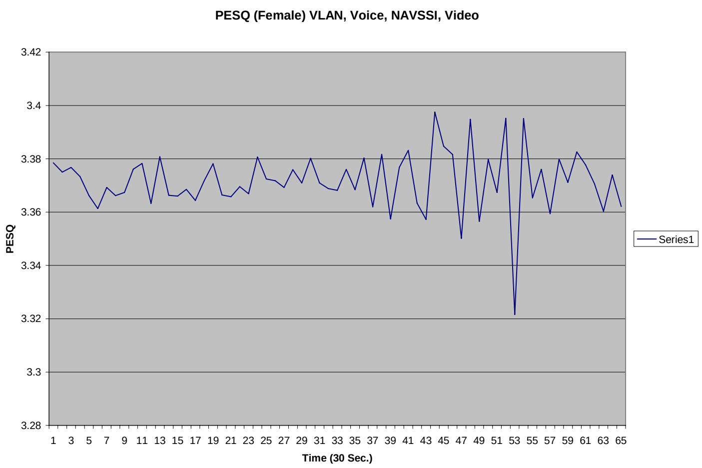
Figure 4-14 Average Jitter (Voice, Navigational, Video, and File Transfer Data)

RTD

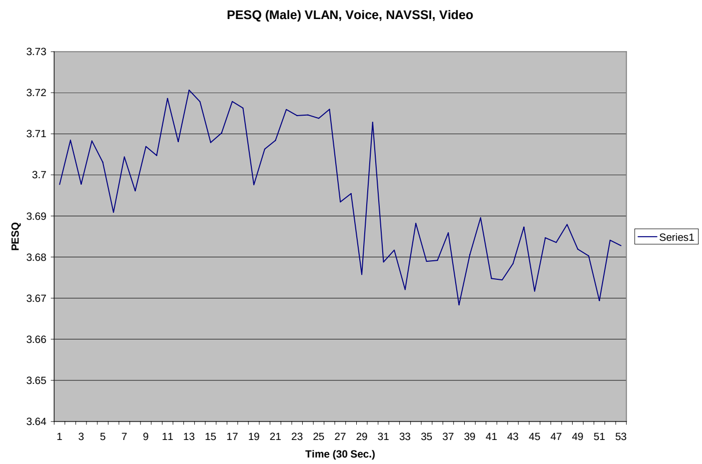
In all scenarios the Round Trip Delay ranged from 136ms to 146ms.

4.1.13.5 Test Condition 2 (VLANs)

VLANs are added as shown in Figures 4-15 and 4-16; Figure 4-16 shows the jitter for VLAN, voice, NAVSSI and video data. Voice, navigational, and video data are run through the network to measure the impact to the PESQ MOS score, Jitter, and RTD of separating Voice, Video, and Data onto different VLAN's.



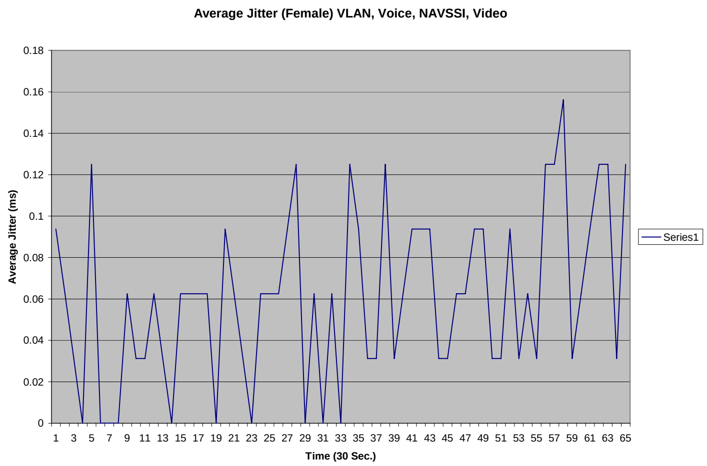
Average = 3.37

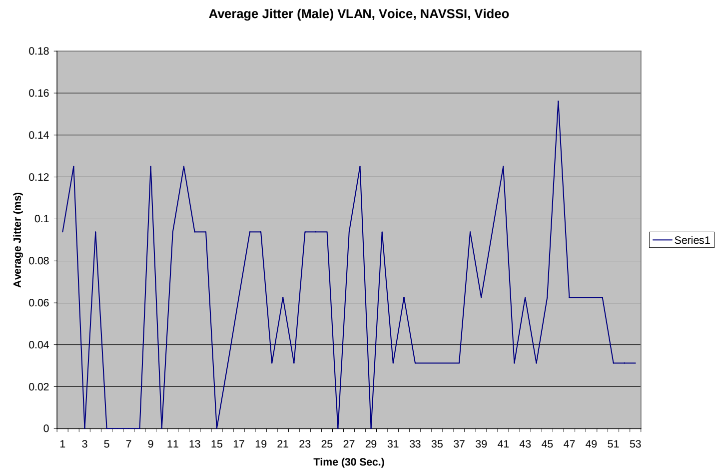


Average = 3.68

Figure 4-15 PESQ Score with VLANs

Note: There is a drop in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.





Average = .0605 ms

Average = .0607 ms

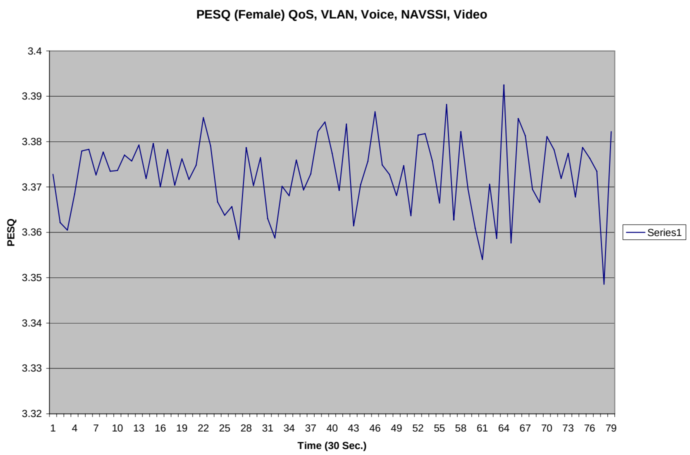
Figure 4-16 Average Jitter with VLANs

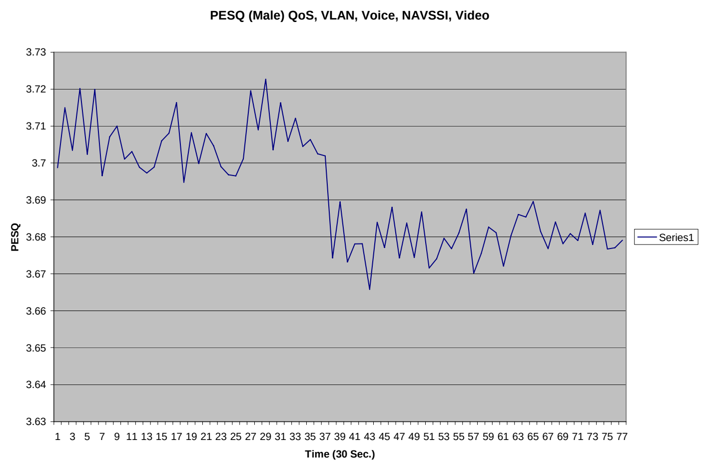
RTD

The Round Trip Delay ranged from 136ms to 146ms.

4.1.13.6 Test Condition 3 (QoS)

QoS is enabled on the edge switch which connects the two IP phones under-test (Figures 4-17 and 4-18). Voice, Navigational, and Video data are run through the network to measure the impact to the PESQ MOS score, Jitter, and RTD of adding QoS to the IP Phone ports. A QoS priority of 5 is set with all other switch ports left at the default value of 0.



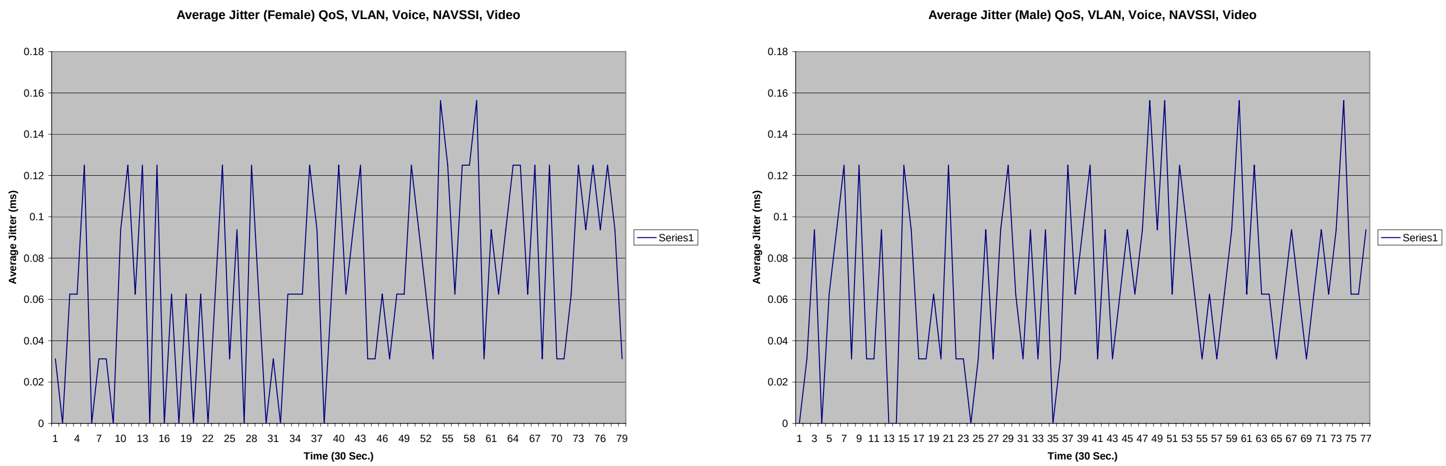


Average = 3.37

Average = 3.69

Figure 4-17 PESQ Scores with QoS and VLANs

Note: There is a drop in PESQ halfway through the male voice shown in the right-hand chart. This is due to the fact that there are two different male files being sent. The second half of the chart are the results of the Male 2 file as opposed to the Male 1 file in the first half.



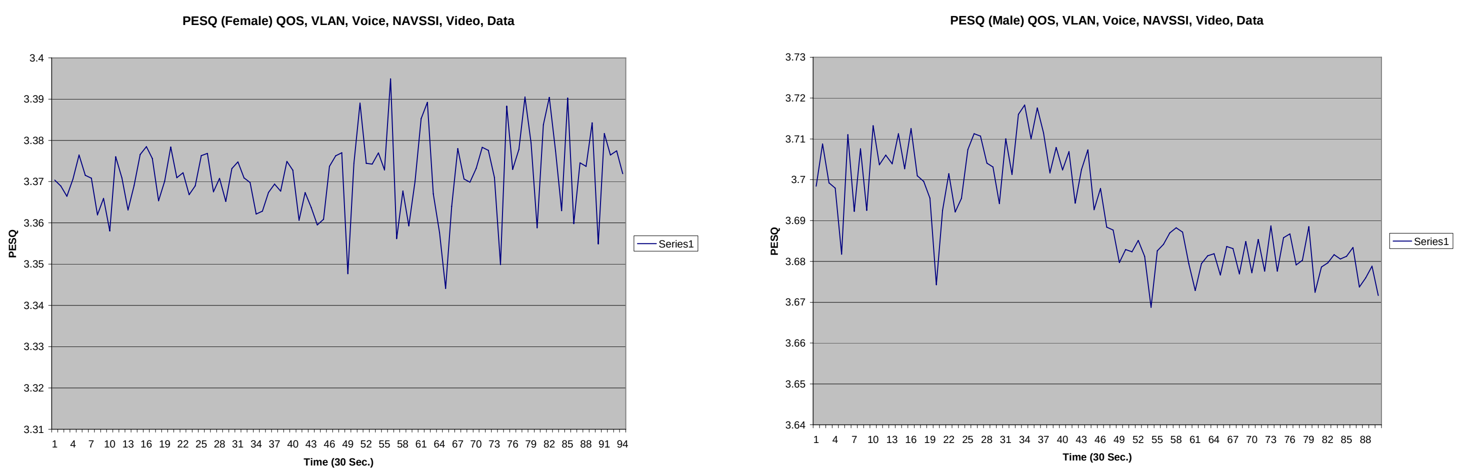
Average = .069 ms

Average = .069 ms

Figure 4-18 PESQ Scores with QoS and VLANs

4.1.13.7 Test Condition 4 (File Transfer Data)

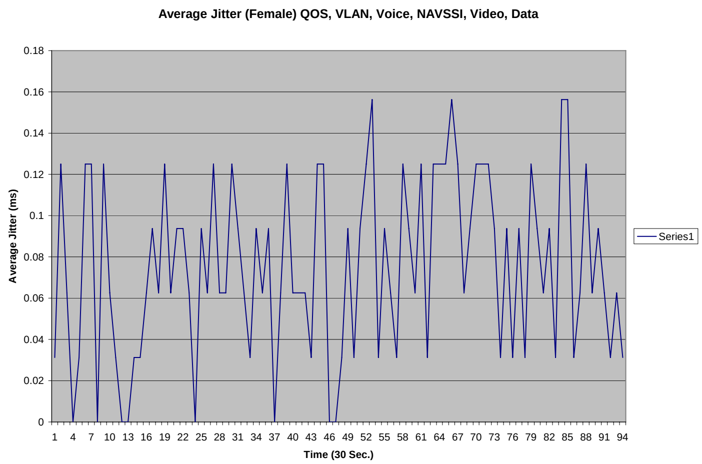
With QoS enabled on edge switch 2 and the VLANs configured, a large file copy was invoked copying data from Server 1 to the Test PC (Figure 4-19 and 4-20). The file transfer occurs on VLAN 50 which is separate from Voice (VLAN 20), Navigational Data (VLAN 40), and Video Data (VLAN 10).



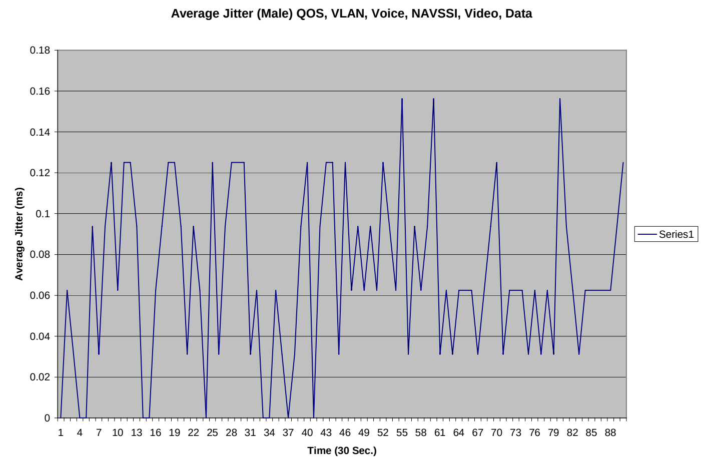
Average = 3.37

Average = 3.69

Figure 4-19 PESQ with QoS, VLANs and File Transfers



Average = .075 ms



Average = .069 ms

Figure 4-20 Average Jitter with VLANs and File Transfers

RTD

The Round Trip Delay ranged from 136ms to 146ms.

4.1.13.8 Switch Performance

Table 4-4 shows the performance of all of the iACT switches under Test Condition 4.

Table 4-4 Switch Performance Chart (1 hr Average)

	CoreSW1	CoreSW2	CoreSW3	CoreSW4	Edge2
CPU	26	25	24	23	29
Memory	69	69	69	68	70

4.1.14 Test Result Summary

4.1.14.1 Observation 1 (Results versus Voice Gender)

In all of the test cases the male voice received a higher MOS rating then did the female voice by approximately 0.3 (Table 4-5).

Table 4-5 Baseline Results versus Voice Gender

Test Condition	PESQ (Female)	PESQ (Male)	Average Jitter (ms) (Female)	Average Jitter (ms) (Male)
Voice Only	3.36	3.68	.074	.078
Voice + NAVSSI	3.36	3.67	.072	.076
Voice + NAVSSI + Video	3.34	3.63	.072	.065

4.1.14.2 Observation 2 (VLAN's versus Baseline)

The addition of VLANs improved the average jitter significantly and had a slight improvement on the PESQ scores when compared to the baseline as can be seen in Table 4-6.

Table 4-6 VLANs versus Baseline

Test Condition	PESQ (Female)	PESQ (Male)	Average Jitter (ms) (Female)	Average Jitter (ms) (Male)
Baseline: (Voice + NAVSSI + Video)	3.34	3.63	.072	.065
VLAN's: (Voice + NAVSSI + Video)	3.37	3.68	12.0	49.8

4.1.15 Conclusion

The objectives of this paragraph are to analyze the concepts and designs covered in the iACT Phase 1 report. The following questions are evaluated.

Question 1: Does the mesh topology (selected in the iACT Phase 1 report) support the requirements for bandwidth and resilience for shipboard use?

Answer: Yes. Through the use of gigabit Ethernet switches and a gigabit backbone there is adequate bandwidth to support voice, video, and data applications running simultaneously. Worst case measurements showed that less then 30% of the CPU and less then 71% of the memory in any of the core/edge switches were used when handling a mixture of voice, video, and data. Also, due to the mesh topology in conjunction with the RSTP Spanning Tree protocol, the network exhibited resilience in the event of a switch failure. RSTP calculates new routes to the destination in the event that the currently used route becomes unavailable.

Question 2: Can the configuration allow voice traffic to maintain quality of service when the network is loaded with lower priority packets?

Answer: Yes. Voice traffic can be assigned a higher priority then other non-voice packets using QoS to maintain quality of service. It is noted that due to the abundance of available network bandwidth in the iACT test bed, quality of service was not an issue, therefore adding QoS to the voice packets did not have a noticeable affect on the end result.

Question 3: Can a scheme be created to allow for all packets on a network to have the right priority that can be implemented in the current technologies?

Answer: Yes. QoS (IEEE 802.1p) provides a scheme which allows for packets on the network to be assigned the right priority. Packets are tagged with a Priority number which differentiates them thereby allowing the network switches to process them before lower priority packets.

Question 4: Does security degrade the over all performance of the network to make VoIP unusable on board ship?

Answer: Not evaluated; because the evaluation criteria was MOS scores between end devices and no COTs devices were found that supported security. The PoC has commercial grade security added into it, but this was commenced at the end of this phase and was not completed, to the level that allowed testing to be done. The final testing needs to have a Secure Communications Interoperability Protocol (SCIP) add with V150.1 so it can be tested with current TDM products. The inclusion of a SCIP device is beyond the scope of this research since this project is unclassified and the use of SCIP products is classified.

4.2 Feasibility of Using Open System and Non-Proprietary Protocols

4.2.1 Introduction

Open and non-proprietary systems go hand in hand in many ways. Open system came into being in the 1980s as Unix competed with the current mainframe and minicomputer manufacturers. This competition continued with operating systems like Microsoft's Windows, which is not an open system because it is owned by Microsoft, and its source code is not available like the many flavors of Linux. This is now tempered by the ability to develop and extend the Windows operating system. It has also been tempered by the ability to run Windows software on hardware manufactured by different companies, with limited issues with compatibility. Non-proprietary software can be open source if it is not owned by an organization or individual. This does not mean that it is not controlled by some kind of license that it must maintain in the open source arena. In some cases, companies will allow use of their proprietary protocol through tools that are purchased from them, or are controlled by them. In many cases the functionality of such tools is limited to a subset of features that the owning company can do with their protocol. Also, the company can make changes to the protocol and is not required to maintain compatibility with the older versions, which can create obsolete products as well as source code that was written with an older version.

We can separate the different types of systems that come from many of the suppliers to the US Armed Forces. All the major telephone vendors have their own proprietary protocols that communicate between their switches and end devices. This becomes apparent when you examine Basic Rate Interface (BRI) implementation between different switch manufacturers, and the changes that were made to support tactical requirements that the military required from the different manufacturers. Several manufacturers are now supporting open system/non-proprietary protocols to support communications between switches and end devices. A few telephony manufacturers are completely open standard – such as the NEC Sphere – Sphericall system, and REDCOM's SLICE 2100 platform - that have gone through the Joint Interoperability Test Command (JITC).

4.2.2 Session Initiation Protocol

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants, without dependency on the type of session that is being established. These sessions include internet telephone calls, multimedia distribution, and multimedia conferences. SIP itself does not participate in the sessions but merely enables and controls them. There are several other protocols that have been developed to do the actual work of carrying the session data.

In recent years the community has chosen SIP as the de-facto signaling protocol for Voice over IP (VoIP) applications. It was designed specifically to be simple and highly extensible. It is this simplicity that makes it the perfect signaling protocol, as it is highly

scalable and independent of media and session type. However, the protocol is still evolving today as the technology matures. Several proposals have been introduced that would provide additional functionality for telephony applications but as of yet they have not been ratified.

Because only a few extensions have been ratified, SIP on its own can only perform a few basic functions as it relates to telephony. It is for this reason that vendors have had to develop their solutions to this problem while they wait for the protocol to mature. However, this does not prevent the use of SIP today. Most solutions available today use SIP for signaling but rely on other protocols, both proprietary and open standard, to complement SIP and thereby achieve the more complex features.

SIP is a request-response protocol that closely resembles two other internet protocols, HTTP and SMTP (the protocols used for the world wide web and email); consequently, SIP sits comfortably alongside internet applications The Session Initiation Protocol (SIP) [1], developed in the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF), takes a different approach to internet telephony signaling by reusing many of the header fields, encoding rules, error codes, and authentication mechanisms of HTTP. Using SIP, telephony becomes another web application and integrates easily into other internet services. SIP is a simple toolkit that service providers can use to build converged voice and multimedia services. It is crucial to understand that other protocols must be used alongside SIP in order to provide complete telephony services.

This report provides only a vague description of the protocol's workings. This description is provided only to place the work into context. A complete description of the components, specific extensions, and modes of operation of SIP is beyond the scope of this paper. For more information please see the protocol standard as defined by the IETF in RFC3261. This RFC obsoletes RFC2543, which was the original SIP specification. RFC3261 defines SIP itself and 6 extensions or methods. The RFC is extended or amended by RFC3265, RFC3853 and RFC4320. These RFCs define additional extensions including SUBSCRIBE, NOTIFY, MESSAGE, INFO, SERVICE, NEGOTIATE and REFER. There are a number of additional RFCs related to SIP but the basic protocol is described by these four.

SIP is becoming the protocol of choice for the application layer for its extensibility, scalability, and adaptability. And, for the same reasons, different SIP extensions indicate different ways of implementing any given service, which is extremely vexing in the user and the vendor community. Relevant SIP protocol suites with extensions should be tested at Department of Defense (DoD) test laboratories and the Defense community should be a major driver for pushing a common, interoperable set of SIP features.

4.2.3 Current Supported Features

Table 4-7 is an abbreviated list of features that are supported by NEC Sphere's Sphericall IP PBX in release 5[22]. JITC-certified Sphericall IP PBX delivers assured connectivity via Multi-Level Precedence and Preemption (MLPP) for special C2 (Command and Control) users including strategic leadership and those who manage strategic assets. They are not on the committee that is tasked with creation of Assured Services SIP (AS-SIP) and their product does not support AS-SIP at this time; they implemented it with RFCs and drafts from the IETF. The list in Table 4-7 is very extensive, compared to the few features that were determined to be need to implemented SIP for the US Navy in the original study.

Table 4-7 Features Supported in Sphericall IP PBX Release 5

General Telephony Services
Call Announce
Call Transfer
Call Coverage: Multi-Level, Follow Me, Conditional
Call forward
Call Hold
Call Waiting
Music-On-Hold
On-Hold Reminder
Dial-Out Authorization Codes
Direct Inward Dial
Direct Outward Dial
Inbound Routing Schedules (Automatic)
Message Waiting Indicators
Multi-Party Conferencing
Park Zones
Pickup Groups
Class Of Service Profiles
Permission Lists: Allow / Disallow Specific Numbers
Trunk Hunt Groups: Directional
User Access Authorization Codes
Automatic Route Selection (ARS)
Call Recording (Optional)
Call Admission Control
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Call Accounting
Call Detail Reporting

[22] http://www.spherecom.com/product_docs/Sphericall_Data_Sheet_53106.pdf

Table 4-7 Features Supported in Sphericall IP PBX Release 5 - Continued

Data Export: Originator ID, Receiver ID, Intended Receiver ID, Time, Duration, Outcome, Reason
Key Industry Standards Support
SIP - RFC 2543 / 3261
MGCP - RFC 2705 / 3149
SIPConnect for SIP Trunking
SIMPLE (Windows Messenger)
TAPI 3.0
DirectX 8.0
SMDI
TCP / IP / UDP
DHCP
FTP / TFTP
SNTP
RTP / RTCP
SOAP
XML
Advanced Communications Features
Call Recording (Optional)
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Softphone for Mobile and Remote Users
User Presence Status Monitoring
*Standard Telephony Features**
Caller ID Display
Call Transfer (Attended or Unattended)
Mute
Hold
Park / Unpark
Do Not Disturb
Transfer to Voice Mail
Redial
Incoming Call Indication with Caller ID
Message Waiting Indication
Missed Call Indication with Caller ID
Multi-Party Audio Conferencing
* Phone/device dependent.

A key group of features were chosen to be reviewed in detail as how they would be implemented in SIP and if the protocol supported the feature directly. The features chosen were ones that were determined as important to an installation on a US Navy

vessel. There were other features which were not evaluated because they were known to be implemented or not required. See *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy Phase 1, Volume I*, for more details on the results of the evaluation.

4.2.4 Shortcomings of SIP

SIP was designed to solve a small but important set of issues and to allow interoperability with a broad spectrum of existing and future IP telephony protocols. To this end SIP provides four basic functions:

1. User Location: mapping a user's name to their current network address (similar to DNS)
2. Feature Negotiation: allows User Agents (UA) to negotiate a common set of features
3. Call participant management: adding, dropping, or transferring participants
4. Modifying session features while a call is in progress.

Any other functions must be performed by other protocols.

Its simplicity means that SIP is not a Session Description Protocol (e.g., SDP) nor is it able to perform conference control functions. It is also not a Resource Reservation Protocol (e.g., RSVP) and it has nothing to do with guaranteeing quality of service (QoS) (e.g., 802.1p, Type of Service (TOS)). SIP can work within a framework with other protocols to insure these roles are played out - but SIP does not perform these functions itself. SIP is regularly deployed alongside SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP, RTP and a variety of other protocols.

Because of the simple nature of SIP many of the functions under study are not achievable with native SIP alone. Standard methods for deploying these features have not yet been ratified due to the myriad of different potential methods to deploy any given feature. Vendors have independently chosen varying methods to solve these issues, which, in turn create a non-interoperable or proprietary situation. Due to this current situation where vendors have not reached agreement (and the lack of standards) it will be many years before multi-vendor solutions with “plug-and-play” advanced features are available to the marketplace. This leads to an environment today where COTS SIP products cannot be guaranteed to interoperate or even have similar feature sets.

4.2.5 Assured Services SIP

Assured Services SIP is defined in the Unified UCR2008. MLPP is the TDM version of assured connectivity, and AS-SIP is the IP signaling protocol for a robust infrastructure. See Chapter 2 for a detailed review of AS-SIP features and functionalities.

4.2.6 Shortcomings of AS-SIP

In many ways AS-SIP does not follow the Open System concept. It is limited currently to a few chosen companies that were selected to participate during the creation of the specification; guided by Computer Sciences Corporation. (www.csc.com) Because of this the information currently is restricted and limited from the open market place. In our work, we have found that it adds to the SIP headers so most servers will ignore the added parameters and use what it can understand, limiting the functionality but making it universally useable with solutions that don't support AS-SIP.

In the current version of the UCR2008, it does not address the end device. In the UCR2008 it allows the end device to be a proprietary protocol. The group that was chosen to guide the specification does not include end-device manufacture. Some of the companies have their own end devices but their concentration is the Local Area Controller (LAC). We have been told that in future releases of the UCR there will be specification for the end device to support AS-SIP. The SIP protocol for trunks and end device is very similar, so it can be interpreted from the UCR and expanded on, see Chapter 3, iACT AS-SIP Communications Terminal Research, for more details on the research of the PoC and AS-SIP .

4.2.7 Trunks Verses End Devices

There are two types of protocols: one that interconnects between switches, and one that interfaces with end devices. In some cases they may be the same, or they may have minor differences. This is important to understand since some companies support the protocol for trunking but not for end devices, or vise versa. They may use a proprietary one for one, and use a non-proprietary one for the other, making things very disconcerted. In some cases they will use an open protocol and add features that make it incompatible with the base protocol, or limit its functionality. This will become important as we start to discuss Assured Services SIP and how different companies choose to implement it.

In the case of Avaya they have implemented AS-SIP in between LACs but use their own proprietary protocol to the end device. In the current UCR2008 this method of support is allowed. In cases of companies like REDCOM they support AS-SIP out to the end devices as well as between LACs. Avaya's trunks support AS-SIP on Call Manager (CM) 4.0 with the JITC patch applied. The inherent problem is that their SIP trunks do not support dial access trunks. The result is that an end device can connect to the trunk and accept calls, but the end device cannot make calls to other end devices. The Avaya

implementation requires the SIP Enablement Server (SES) to process SIP calls. In future builds the SES will be integrated into the CM and this limitation will be removed. At this time the SES has not and is not planned to be sent to JITC for testing. This resulted in the Proof-of-Concept IP Communications Terminal not being included in the Trident Warrior 2009 exercises.

4.2.8 Open Source

It was recently reported in Government Computer News Volume 1 Number 1, "Pentagon: Open source good to go" by Joab Jackson, http://www.gcn.com/online/vol1_no1/47320-1.html, that Open Source may be allowed into the military. The military has been using Apache, Perl, Linux and several other open source programs but it has always been a grey area. Daniel Risacher, the data strategy leader for the Office of Secretary of Defense, is working on a draft of a memo to be released in November of 2008. This will replace the last several memos that have addressed different issues with using open source. Daniel sees open source in three different lights:

1. The body of code, and the resulting software, is freely available,
2. The methodology of volunteer developers off-set the cost of development,
3. The licensing is less restrictive than proprietary software.

These three points result in the following benefits to the armed forces as well as other government agencies:

1. Ability to update the source when a problem is found, in a timely manner,
2. Faster prototyping,
3. Reduced overall costs for the life of the application.

4.2.9 Conclusion

It depends, in the end, on how to classify AS-SIP. SIP with some of the drafts ratified could come very close to the requirements. AS-SIP takes that next step, and rounds out the need for communications in a tactical environment. Since AS-SIP is being supported by multiple companies and will be released and be available, it should fall into the open and non-proprietary system classification. This will open the door for other companies, and keep the government from being restricted to a single vendor. The introduction of open source into the equation will make the communications system "open system", if the armed forces decide to implement current open source projects and add the support for AS-SIP. Refer to *Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy Phase 1, Volume I*, for a detailed review of Open Source projects and the licensing methods currently used. The combination of AS-SIP and Open Source could result in a very flexible solution that can be updated and distributed throughout the full government infrastructure.

4.3 Feasibility of Wireless Phones

4.3.1 Introduction

Communications on a vessel are critical. To this end the ability of sailors to be mobile and still have the same connectivity as at a stationary phone is also critical to empowering the sailor. Currently, the sailor carries a larger radio which has limits on its functionality and which is also costly (handsets, transmitters/repeaters, and the antenna system in place on the vessel directly impact cost and weight). Phase 1 of this Technical Report evaluated several different technologies and wireless fidelity (Wi-Fi) was noted as the best overall solution at the time. This is not to say that Wi-Fi does not have shortcomings; but they were lesser in number than other technologies that were reviewed. We implemented and evaluated a Wi-Fi network built around Aruba[23] network components and Ascom[24] Wi-Fi phones.

4.3.1.1 Set Up of the Wireless Network

Aruba Networks was chosen for the wireless infrastructure; they were the only vendor that was Federal Information Processing Standard (FIPS) certified. The access points (AP) are light (*light* is defined as the processing is done by another unit) and are managed by a central controller. In the original implementation of Wi-Fi, heavy AP (*heavy* is defined as the unit does its own processing independent of any other device) were used that were all separate, and that required clients to be handed off between APs and re-authenticated for each individual AP. Also within this heavy AP framework, each AP needs to be configured separately, which is time-consuming if a key, or other configuration parameter, requires changing.

In a light AP framework, each AP is controlled by the central controller, which manages the system after installation. Because the central controller is administrating security, there are no hand-offs between the APs, which is critical to avoid dropping VoIP calls. Adaptive Radio Management, (ARM) manages the AP in the area of power and client connectivity. Meru Networks[25] also makes a central controller which is similar to Aruba Networks, and calls their product "Air Traffic Control" - both products do the same kind of management of the AP. ARM makes provisions for voice clients and stops several of the management functions when a voice client is connected to an AP, until the client moves to a different AP. Ascom however, does not recommend this type of management for their wireless phones because of problems in the field in the past.

---

[23] Aruba Networks – 1344 Crossman Avenue, Sunnyvale, CA 94089 P408:227:4500 www.arubanetworks.com

[24] Ascom (US) Inc. 598 Airport Blvd., Suite 300 Morrisville, NC 27560 P:919.234.2470 www.ascomwireless.com

[25] Meru Networks – 894 Ross Drive, Sunnyvale CA 94089P:408.215.5300 www.erunetworks.com

Two of the APs are distributed inside the lab area, resulting in overlap of the two signals; the controller placed one at channel 1 and the other at channel 6. The third AP, which the controller placed on channel 11, is located on the other side of the wall to allow testing from within the manufacturing areas.

4.3.1.2 Security of the Wireless Network

Security is limited by the end devices that are connected to the network. The devices chosen were Ascom i75 phones and an Axis camera. These two type of devices supported Wi-Fi Protected Access Version 2 (WPA2), and Pre-Shared Key (PSK) with Advanced Encryption Standard-Counter with CBC MAC (AES-CCM) resulting in WPA2-PSK. WPA2-PSK is a preferred algorithm over WPA-PSK because the Temporal Key Integrity Protocol (TKIP) encryption algorithm has been replaced with AES. The addition of an authentication server such as a Remote Authentication Dial-In User Server (RADIUS) or a Virtual Private Network (VPN), requires the client to run a special client code that, in most cases, requires user intervention.

4.3.1.3 Set Up of VoIP on the Wireless Network

The set up of the wireless network started with the Aruba network - without this the Ascom handsets would have nothing with which to connect. We began with the MC-200 (Figure 4-21) which is a FIPS certified unit. It is a small unit for a small office only supporting 6 access points, but its operating system, Aruba Mobility controllers Base OS (ArubaOS) and Adaptive Radio Management (ARM) is the same throughout the product line. The MC-200 has many features that were not explored within this study, such as a built-in firewall. The wireless security was not exhaustively tested in this study (however, Aruba already completed this testing when applying for the FIPS certification). After the MC-200 is set up, it finds the individual access points for the administrator to place into the group.

4.3.1.4 Ascom and Aruba Equipment

The initial process was to determine what phones we would use for the evaluation. After looking at the major vendors, the Ascom i75 phones stood out as feature-rich (and also supported RFC-SIP). Their product line falls into several different components that would add to the feature richness of the complete system.

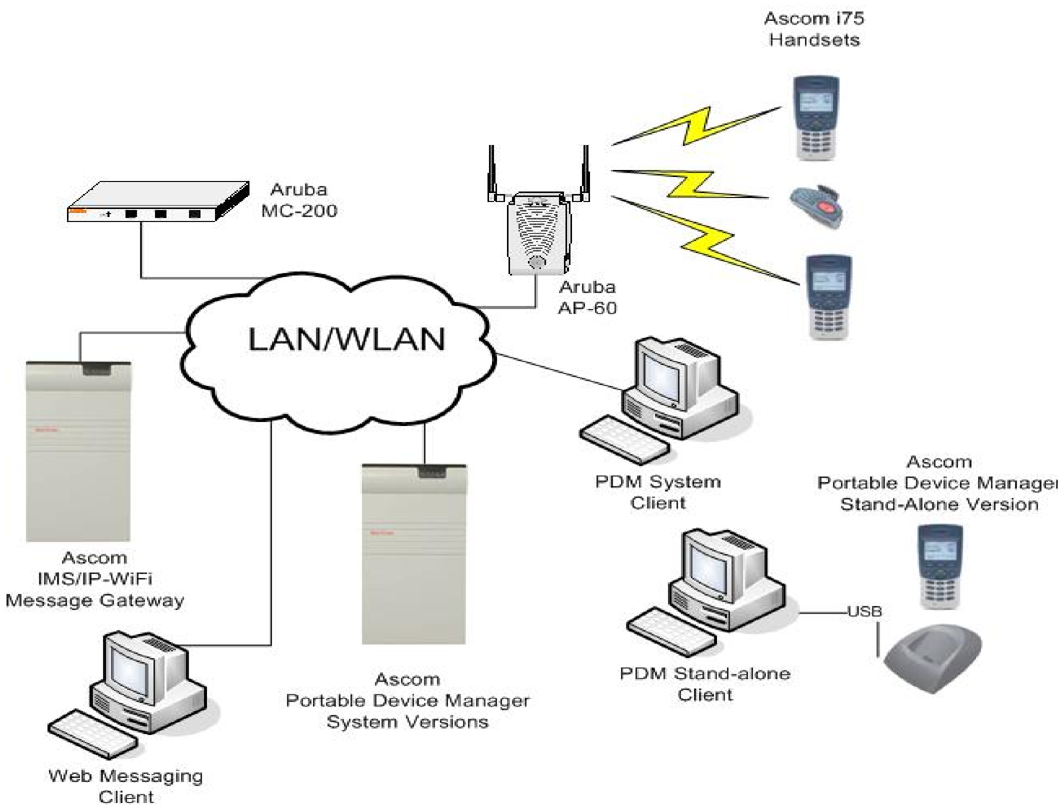


Figure 4-21 Aruba Network with MC-200

4.3.1.5 Ascom Portable Device Manager

The first important product that made Ascom unique was their Portable Device Manager (PDM) which is based on their UNITE product line of Linux appliance servers. The PDM allows the phones to retrieve the profiles of the person or station that logs into it, thereby reducing the need for dedicated devices and the number of units required. When the device is turned on, it will request the login and password, and then retrieve that configuration and sets of features, like speed dials and configuration preferences. Each profile is managed from a central web-based tool that allows a thousand-plus configurations to be adjusted and saved into different profiles. There is also a stand-alone version for configuring the handsets out of the box, or if you are only using a few and do not require the push of features or the ability to change profiles via log-in at the handset. The PDM also directs changes to the different handsets, so they are remotely updated as soon as any changes are made on the web interface.

4.3.1.6 Ascom Integrated Message Server

The Ascom Integrated Message Server (IMS/IP-WiFi), which should not be confused with IP Multimedia Subsystem that is a powerful emerging technology, incorporates many of the same types of features but in a non-proprietary format. The IMS/IP-WiFi is a part of the Ascom solution that acts as a messaging gateway and controls the alarms

between the messaging system and the handsets. It also allows individuals from a PC to log into a web-based paging system and send messages to the individual handsets from anywhere on the WLAN that can access the resources (and has the credentials). An application called Basic Alarm Manager is included in the IMS/IP-WiFi. This application makes it possible to send messages to handsets in the system, or activate outputs in the system as a reaction to activated inputs, alarm or user data from handsets in the system. Examples of this feature are: the end user can press a button on the phone and have a message sent to other defined phones in a group. The phones also has the capability to send a automatic message if the phone is not moving for a defined length of time.
A phonebook that can be accessed from the wireless handsets is also included in the IMS/IP-WiFi. Phonebook service is delivered along with the IMS/IP-WiFi, and gives the same functionality as the IMS/IP-WiFi Phonebook (needed for large phonebooks).

4.3.1.7 Phones

The Ascom i75 phones are a highly configurable phone with many features that this study did not use or evaluate. The handsets are said to handle water spray, but are only rated for IP40 and EN 60529. They have been fall tested to IEC 60068-2-32 Ed procedure 1.

The handset has several encryption methods: 802.11i, 64/128 bits WEP, TKIP, and AES-CCMP. These are complimented by several authentication methods: 802.1x, original 802.11 open/shared key authentication, WPA-PSK, WPA2-PSK, LEAP, PEAP-MSCHAPv2 and EAP-MD5. It is then enhanced with Pre-authentication, PMKSA cashing and CCKM. For our testing we set up the Aruba network with WPA2-PSK authentication and AES-CCMP encryption. This combination resulted in a good level of security, which could then be enhanced with the use of a RADIUS server.

The Ascom handsets are extensions off of the Avaya switch, allowing them to connect to any other phone or device that is connected to the Avaya switch. The configuration of the SIP Enablement Server proved to be difficult for the vendor for set up of all the SIP phones, but after completion the Ascom phones worked fine. They support several of the major SIP RFCs: RFC1889, RFC2327, RFC2833, RFC3261, RFC3264, RFC3265, RFC3515 and RFC3842. They also support H.323 with supplementary services, H.450.1-4, and H.450.6-9.

4.3.1.8 Ascom Phone Setup

The Ascom handsets have a two-step process for configuration. The first step, with the Portable Device Manager (PDM) Stand-alone version, places the basic network configuration for each phone onto the network (Figure 4-22). Information can be added to make them unique. This is a quick process, and the PMS System version is used to push the profiles to each handset (profiles that are pushed, only push the designated information and not the complete profile). In the profile under the **Device | General,** select *Phone Mode* and set it to *shared***,** this will have the phone at startup require that the handset be logged into when it is turned on.

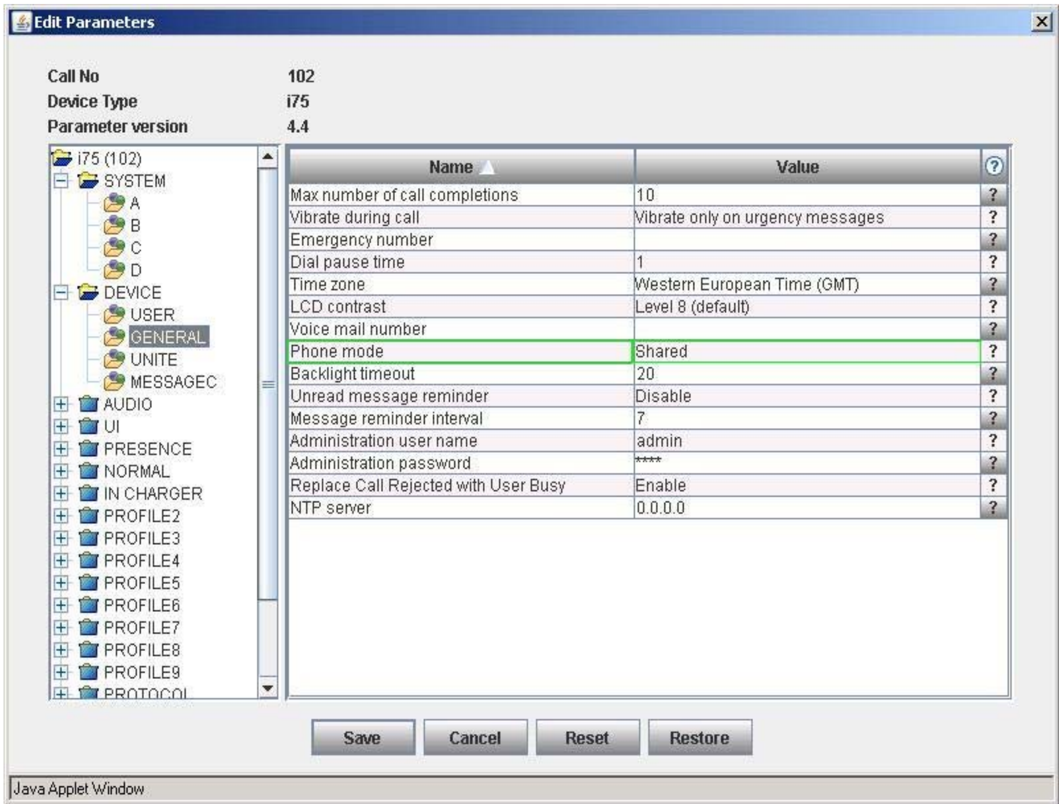


Figure 4-22 PDM Configuration Screen for Device Settings

4.3.2 Wireless in a "Tin Can"

One of the largest unknowns for wireless technology is the ability to work within a metal enclosure. Different companies have shown concern for this environment, but both Meru Networks and Aruba felt that with their equipment any problems could be circumvented. Another company, InnerWireless[26], provides a unified wireless platform – a passive wireless distribution system – as the foundation for wireless environment. This platform is considered the most reliable of its kind – there has never been an operational failure of this passive system. The platform is a coaxial-based, neutral host, broadband antenna system designed for the transmission of multiple RF signals simultaneously over a passive antenna infrastructure. MobileAccess Networks[27] uses the same distributed system that makes RF management easier, and incorporates it into a single system that is wired once. The core can then be reused as new technologies are added (Figure 4-23).

[26] InnerWireless – 1155 Kas Drive Suite 200, Richardson TX 75081 P:972.479.9898 www.innerwireless.com

[27] *Universal Wireless Infrastructure Structure*, MobileAccess Networks Interior Communications Voice Symposium December 3, 2009 http://icvoicesymposium.com/Presentations/Wednesday/10_Universal Wireless Infrastructure_MobileAccess Networks.pdf , Mobile Access Networks – 8391 Old Courthouse Road, Vienna, VA P: 866.431.9266 www.mobileaccessnetworks.com

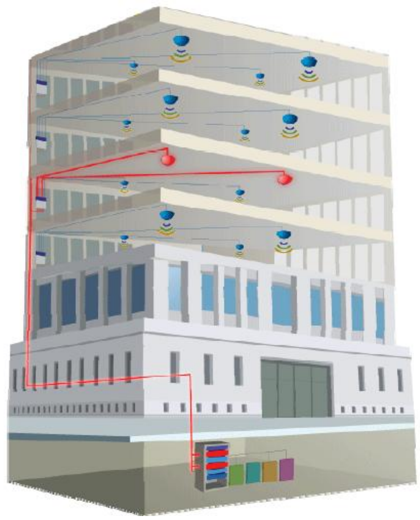


Figure 4-23 Distributed System with RF Management

There are several groups that are working on different mobile communications for US Navy vessels. Work has also been done at a few of the different ship yards. The groups have not responded to requests for information for the iACT program. Since these groups have access to the vessels, examination and evaluation was not done within this program.

During SPAWARs Interior Communications Voice Symposium in December 2008, J. Don Pierce of NAVSEA 05W43 (james.d.pierce1@navy.mil) gave a presentation called "E^3 and Spectrum Wireless Challenges"[28].

During his 23-slide presentation, he covered many of the difficulties of implementing wireless technology and the methods to resolve them. His primary message was to contact his group before planning on installing wireless technology on a vessel, and work with his group to implement it the first time correctly. Don has found that changing a system already installed is more costly than working with his group to develop the system up front, prior to purchase and installation of a wireless system.

[28] *E^3 and Spectrum Wireless Challenges*, Interior Communications Voice Symposium December 3, 2009 J. Don Pierce NAVSEA 05W43, james.d.pierce1@navy.mil , http://icvoicesymposium.com/Presentations/Wednesday/6_Wireless Spectrum and E3 Challenges_Don Pierce.pdf

They are also able to measure the internal reflection of the compartments and determine leakage that can be dangerous to other devices on the vessel.

4.3.2.1 Bandwidth and Access Points

Even if the wireless handsets are located on the same AP, the traffic is directed at the MC-200 and is placed on the wire. This creates traffic that could be maintained at the AP. Figure 4-24 is a Wireshark capture of a call, followed by Figure 4-25 and Figure 4-26 which is the information that the MC-200 stored. This functionality is what allows the calls to be maintained during the transfer between AP as the sailor transverses the vessel.

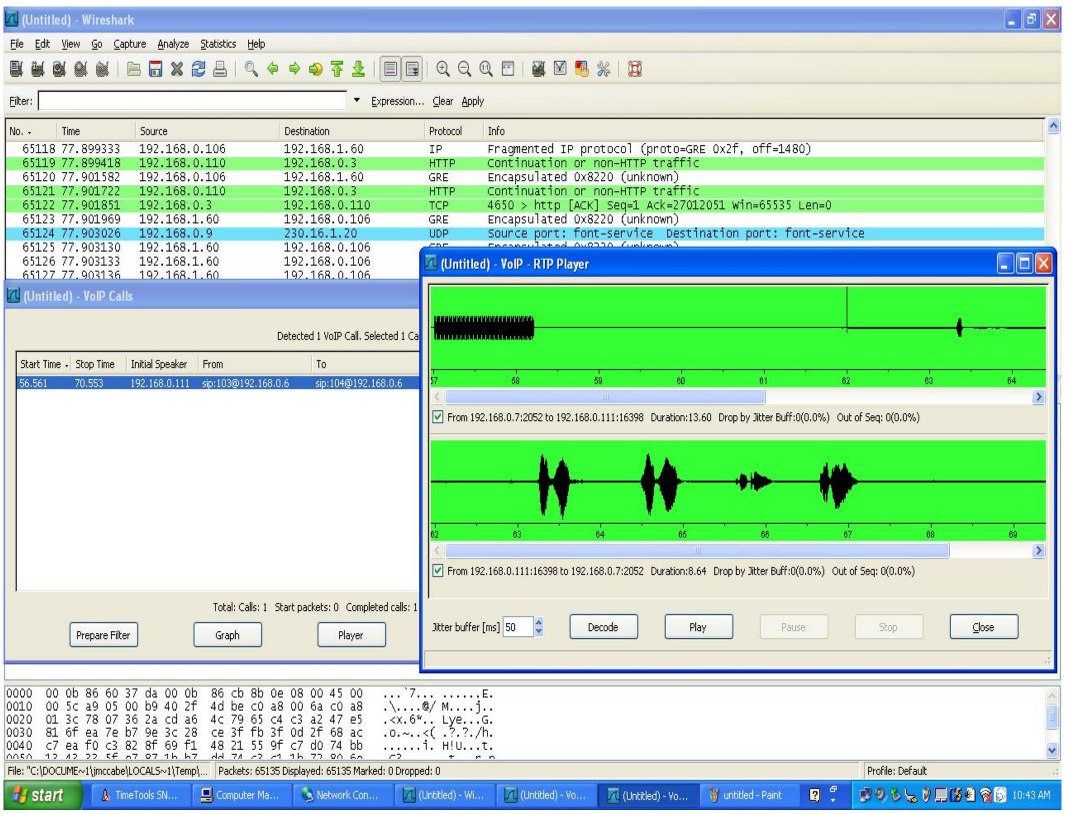


Figure 4-24 Wireshark SIP Call Between Ascom Phones

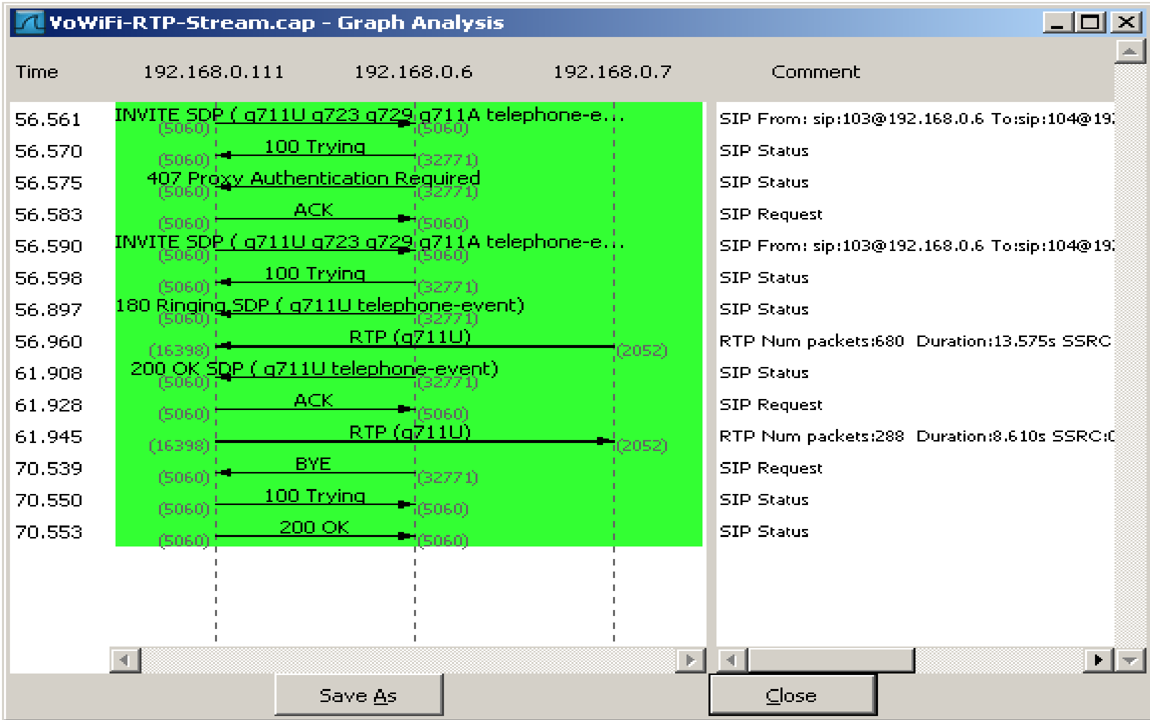


Figure 4-25 Wireshark SIP Call Details Between Ascom Phone

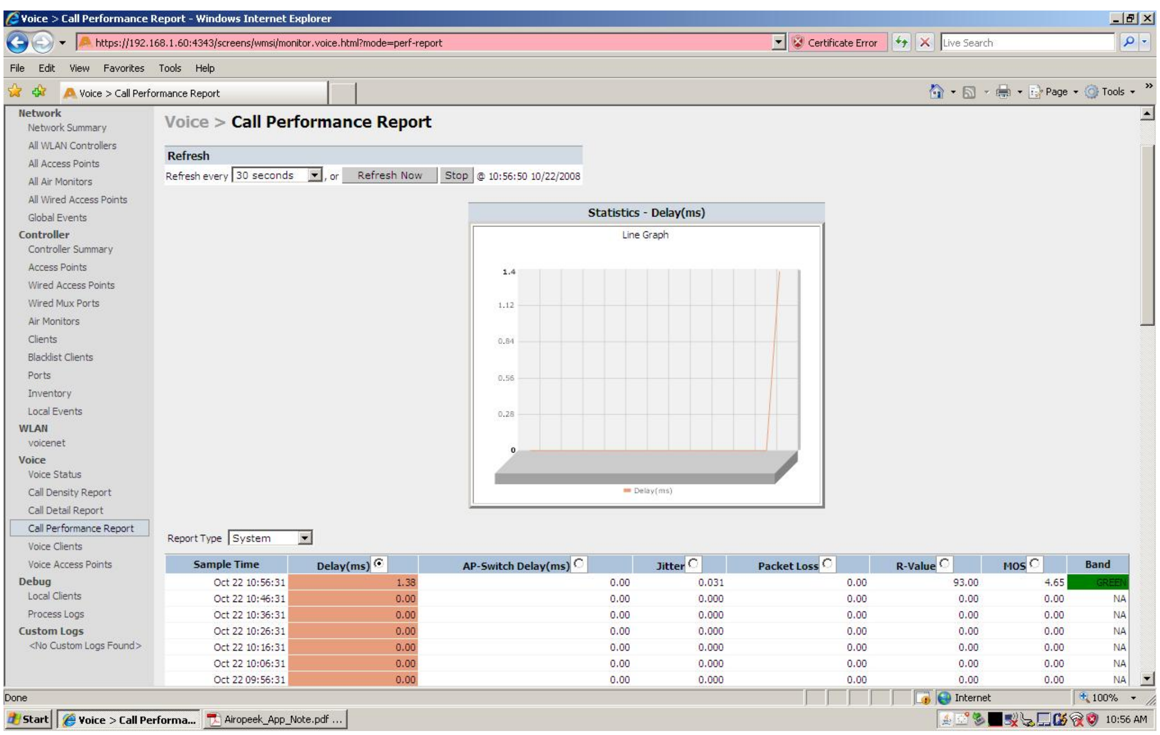


Figure 4-26 Aruba MC-200 SIP Call Between Ascom Phones

The MOS score shown in the Aruba web pages is high compared to GL Communications (Figure 4-27). So there is no reduction of bandwidth since all the packets are passed back and forth from the MC-200. With three AP active and the single call being processed here is the summary of traffic at the MC-200 port.

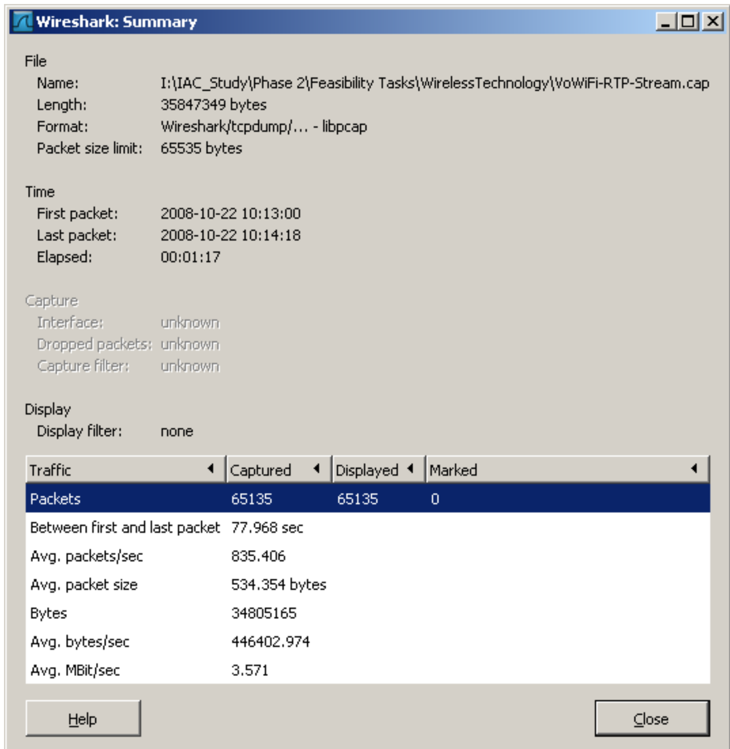


Figure 4-27 Summary of SIP Call at MC-200 Port

Wireless currently does not have any devices that support AS-SIP, since this specification does not include end devices at this time. In the future the specification will cover end devices and at that time manufacturers will start to evaluate adding it to their products lines.

4.3.2.2 Wi-Fi vs. WIFCOM

Even though these two technologies accomplish the same function, wireless gives the sailor more features for less cost. WIFCOM comes in two different configurations: “trunked” and “non-trunked”. Trunked gives the sailor the ability to call separate radio handsets, with some granularity, but at an added cost and complexity. Non-trunked has no ability to call individual radio handsets but it is a major cost reduction from a trunked system. In the case of Wi-Fi, it gives the sailor the ability to have a desk phone at all times. It has its own call lists as well as system call lists -avoiding the need to know the sequence to call another sailor or position - only the extension, or the ability to look it up in the call lists. It also integrates to the phone system to determine if the phone (and its

login) has voice mail on the PBX. In the case of Ascom, it also has the alarms and the ability to text message the different handsets using the extension or the call lists. WIFCOM has some advantages that will lessen with time. The radio handsets are rated for IP60 where the Ascom is only IP40, but the cost is less so they can be replaced a few times before the cost of a radio handset is reached, and even more times if it is a trunked handset. The wireless manufacturers are watching as the market grows and determining the options that are required in the field. Recently, one company released an intrinsically safe wireless handset. The Wi-Fi based systems also allow tracking of the end devices related to the APs. Applications are available that place the end device on a map of the vessel. These applications can also maintain a history of the location of the end devices. This allows verification that the end device has made its rounds on a schedule, and shows any anomalies.

4.3.3 Conclusion

In conclusion, wireless technology is improving all the time. Specifications for equipment researched for Phase 1 have improved in several ways, primarily battery life, features, and the ability to integrate with SIP PBXs. Wireless technology is currently being tested by several military groups (no official word has yet been received on results). Vendors sound very positive on the results, but they are not able to go into details on the work that they are doing with the different military groups. Systems like Aruba are listed as FIPS certified. As well as the coaxial-based, neutral host, broadband antenna system designed for the transmission of multiple Radio Frequency (RF) signals simultaneously over a passive antenna infrastructure, technologies like InnerWireless and MobileAccess Networks should help to resolve the issues of implementing the system on surface as well as submerged vessels. With the forward motion of the technology, the current testing in the Navy, FIPS certified systems, and the vast features that wireless brings to the vessel; it shows a technology that should be continued to be evaluated. This is enhanced with the ability for the base system to map and maintain a history of the end devices.

From our testing, and recommendations from the different vendors, the population on each AP is critical to quality of service. There are several factures that are required in developing the wireless network for quality of service. The use of centrally controlled AP lends to managing the resources and users, to load balance the AP to client utilization. The wireless phones are feature-rich compared to WIFCOM radio. The Wi-Fi phones are close to the same functionality as if the sailor were walking around with a desk phone. While pushing profiles to the individual wireless phone and reducing the number of phones, it still maintains the ability to have the mobile phone customized to the individual user. As the different vendors start to support AS-SIP, this will add to the over all system ability to do priority routing and MLPP that is not found in the current WIFCOM system.

It is time for a Working Group to be created to bring all the various groups together and combine the results and efforts into a single direction that would benefit every group, and move wireless forward on US Navy vessels.

4.4 Feasibility of Reliability and Maintainability

4.4.1 Introduction

Bandwidth issues have been discussed from both the on-vessel as well as the off-vessel perspective. Rear Admiral Brad Hicks, Director of Aegis Ballistic Missile Defense, stated at the Surface Navy Association 2009 Symposium in Arlington, Virginia: "I'm getting tired of getting my butt kicked in the joint arena because we don't have adequate command and control bandwidth and robustness in our communication system," as well as, "We are disadvantaged in the joint fight [in that] we don't have enough bandwidth and we can't get all the data to the ship or off the ship." According to Vice Admiral Mark Edwards, former Deputy Chief of Naval Operations for Communications Networks (N6), the lack of bandwidth capacity on the DDG-51 destroyers and the CG-47 cruisers has been a long-standing problem.

The Total Ship Computing Environment (TSCE) must be reliable and maintainable by the sailors on the vessels. This would include both tactical and administrative networks as well as communications. The network infrastructure is the most important part of the complete system. If the network is not engineered to support the requirements of the end devices that will be connected to it, reliability will never be achieved. Only after the network is designed for reliability will maintainability be achieved. In the current topologies of segregated networks with each requirement separated on its own network, to the PMW-160/ C4I Consolidated Afloat Networks and Enterprise Services (CANES) direction of integrating all the requirements into a single network, the design is critical to the networks ability to handle traffic, and limit jitter and packet loss.

Once the network is designed correctly, then the protocols it supports will also need to be engineered accordingly so as not to produce "denial of access" and/or traffic issues caused by interactions or bad code in individual protocols, or in unison with others. This also applies to the end devices - whether a computer, IP telephone or a bar code scanner, they all need to be engineered into the network so as to extend the reliability of the networks. Media gateways are used to connect end devices that do not support a direct interface to an IP network. This method of connecting end devices to the IP network has limitations that need to be understood in order for them to add to, and not reduce, the reliability and maintainability of the network.

4.4.2 Network Challenges

The network is a critical part of the Voice-over-Internet Protocol (VoIP) system since it is the carrier of voice and contains the Real-time Transport Protocol (RTP) stream. At present there are many different networks - some are IP based and others are proprietary to the data that it carries. In order to address these challenges, the Navy C4I Program Executive Officer (PEO C4I) developed a phased plan to migrate its primary network programs onto a single over-arching program called Consolidated Afloat Networks and Enterprise Services, or CANES (this paragraph is adapted from the "Navy C4I Open Architecture Strategy" for its discussion of CANES). CANES will have at its roots the

Integrated Shipboard Network System, but will also incorporate the capabilities of other networks such as Combined Enterprise Regional Information Exchange System, which is used for coalition communications; the Sensitive Compartmented Intelligence Local Area Network (LAN), which is the shipboard network for special intelligence and crypto logic tactical communications; and the submarine LAN, which is the submarine fleet primary network.

The basic concept of CANES is to take hardware requirements and create a single consolidated computing environment using standard network infrastructure and common rack architecture. Enterprise services will support hosting of both war fighting and administrative application programs. This evolution requires detailed technical exchanges between the program's engineers and a significant amount of resource reprogramming.

The expected benefits of conducting this network infrastructure transformation are to:

- Reduce the number of installs,
- Reduce the physical footprint,
- Allow dynamic sharing of storage and processing,
- Allow more efficient use of computing power,
- Improve configuration management,
- Enhance security,
- Reduce non-recurring engineering costs, and
- Reduce manpower and training requirements.

PEO C4I is working with the Navy's PEO Enterprise Information System to achieve more consistent standards and commonality with the future shore-based network program, Next Generation Network. In addition, the program plans to leverage as much Joint capability as possible, to include the Net-Centric Enterprise Services program managed by the Defense Information Systems Agency (DISA).

Finally, the CANES solution also solves a significant configuration management and supportability problem. Currently, each ship has a different configuration of hardware and applications. Training sailors aboard ship to operate and maintain all of the systems increases the complexity and total ownership costs to the Navy. By moving to a common configuration for hardware and enterprise services, trained sailors can operate and maintain CANES regardless of ship class.

4.4.3 Dual-Redundant Mesh Network

The dual-redundant mesh network is the fourth major evolution in a line of digital networks, designed primarily to support critical control system communications in Navy ships. The first in the line was the Data Multiplex System (DMS) of the late 1970s. In the early 1980s, a fiber-optic upgrade of DMS was developed, the Expanded Service Shipboard Data Multiplex System (ES-SDMS). This was followed by the first packet-switched version of DMS, the Fiber-Optic Data Multiplex System (FODMS), in the late

1980s, and an Asynchronous Transfer Mode (ATM) version of FODMS in the mid 1990s (lab model only). The dual-redundant mesh network evolved directly from FODMS and ATM-FODMS, in the early 2000s. These DMS families of networks (Figure 4-28) share the same design philosophies.

Figure 4-28 Control Systems Operation Over DMS

They also support multiple signal types and data protocols for end system connectivity, allowing otherwise incompatible attached systems to intercommunicate in a fully networked environment. Supported signals include Internet Protocol (IP) over Ethernet, industrial serial RS-232, RS-422, and RS-485, parallel and low level serial MIL-STD-1397 (Type A, B, and E), NATO serial STANAG 4156, synchro 60 Hz and 400 Hz, tri-level discrete (supervised discrete), voltage level discrete (logic level, LED driver, relay driver), and contact closure discrete (up to 115 VAC).

Connection between end systems and the network is provided by interface cards housed in Input Output Units (IOUs), the main nodes of these networks. The IOUs are interconnected redundantly, through a system of actively redundant backbone networks. While the IOU is fully compatible with IP host devices, a second type of system node, the IP Interface Unit (IIU), is optimized specifically for IP hosts, increasing throughput to over 600 Mb/s, for each IIU.

The dual-redundant mesh network backbone networks are currently single-mode fiber-optic 1 Gb/s Ethernet mesh networks (IEEE 1000BASE-LX), upgradeable to 10 Gb/s Ethernet (IEEE 10GBASE-LW). Each mesh runs the Rapid Spanning Tree Protocol, IEEE Standard 802.1D-2004, to ensure fast recovery of each redundant network, in the event of switch or link failures in that network. During the 10s of milliseconds needed for recovery, the redundant backbone continues to support glitch-free operation of DRMN.

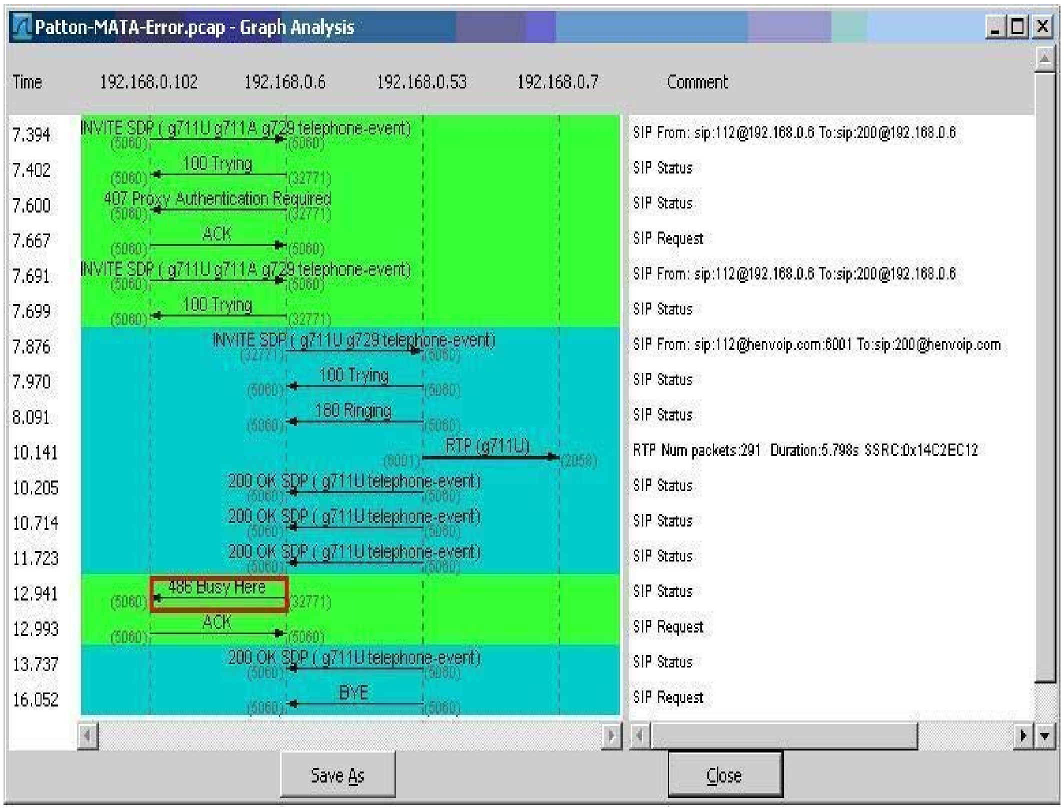
Over the backbone networks, FODMS and the dual-redundant mesh network use two types of active redundancy protocol, both optimized throughout for low latency message transfer. These protocols transmit data packets simultaneously through both backbone

networks. At the receiving side of the data path, the first arrival is used, and any copy discarded. The active redundancy protocols can be used in conjunction with Virtual Local Area Network (VLAN) protocol IEEE 802.1Q, to provide service differentiation of traffic categories through IOUs, IIUs, and the backbone networks.

A Maintenance Group provides constant performance monitoring and fault localization to the individual replaceable card level, message examination by a system operator, automatic downloads of system firmware updates for attached nodes, and an electronic technical manual.

4.4.4 Media Gateways

In the Feasibility Lab we have worked with different media gateways to attach to several different older technologies such as analog phones, BRI phones, IVUT, announcing systems and sound-powered telephone. At first this task looked to be an easy one to complete; however, as each unit was connected to the network and tested, none of them worked out-of-the-box. The initial testing was all done on the Avaya PBX. Several of them required firmware upgrades to even register to the Avaya SIP registration server, and one had to be exchanged with the manufacturer in order to be compatible with the Avaya Communications Manager. The configuration was challenging, and the Patton units had a very hard interface to program. It was very flexible because of its complicated interfacing of several objects that were then related to each other, creating the final result. Many of the problems may have originated from the Avaya SIP Enablement Service (SES), which is an add-on program that handles the SIP externally from the Communications Manager. Several devices were then tested against a SIPx and Asterisk server had worked. One issue that came up was a "busy" being sent from the Avaya to the calling user agent, when the called user agent came off hook, as shown in Figure 4-29. No resolution was found with the media gateway vendors' and it needed to be escalated to Avaya Support for resolution.



192.168.0.102 – Polycom phone
192.168.0.6 – Avaya
192.168.0.53 – Media Gateway
192.168.0.7 – Avaya

Figure 4-29 Patton-MATA-Error.pcap Window

4.4.4.1 SmartLink Micro –ATA Evaluation

Of the three Patton media gateways evaluated, the SmartLink Micro – ATA was an easy device to configure (Figure 4-30). Patton support was helpful but did not follow through on cases with resolution to the problems. Other Patton media gateways were configured through web pages that could export a configuration file that could be edited and then imported back into the unit. The configuration language was well documented in a 600-plus page manual that was organized by object. It was found that the base configuration done by the web interface, and then the configuration file to complete the configuration, was the best approach.

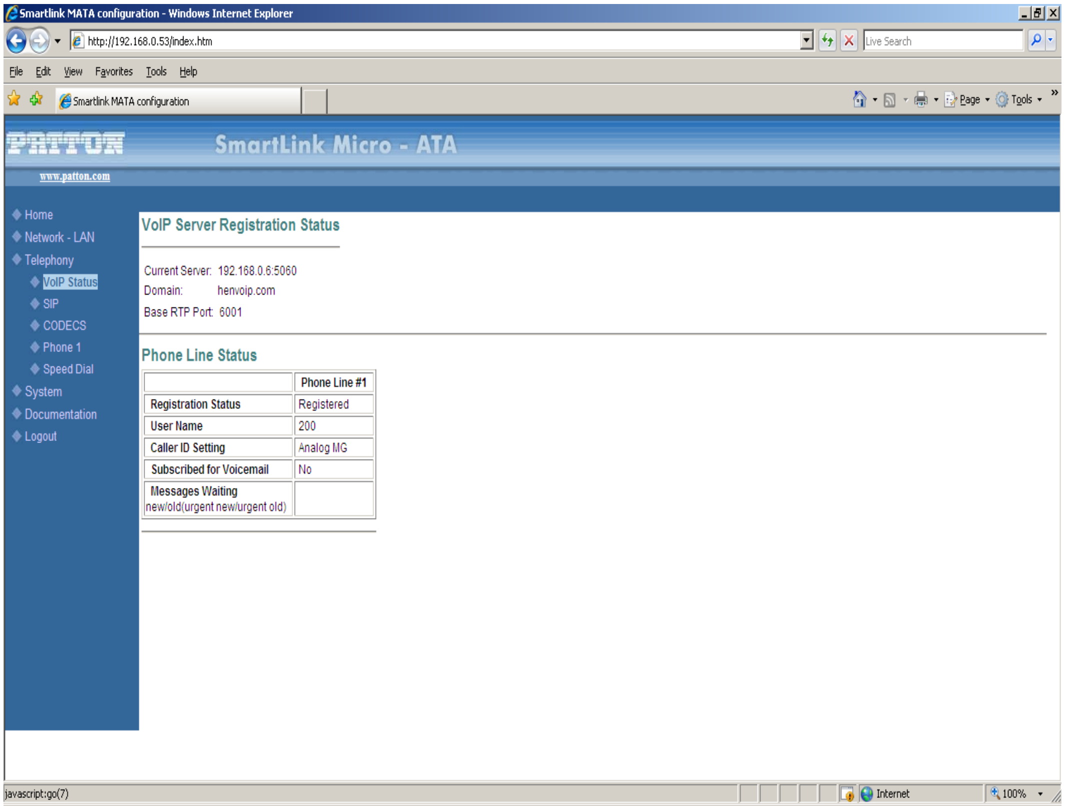


Figure 4-30 Patton SmartLink – ATA Window

4.4.4.2 Multitech MultiVoIP Evaluation

The Multitech MultiVoIP unit was purchased first as a SIP media gateway (after extensive work with Support) but it was determined that it was not compatible with the Avaya Communications Manager and a special version was required. The Avaya Communication Manager version was not SIP-based, but was based on H323 and tightly integrated with the Communication Manager. This limits the media gateway work with a set version of the Avaya Communications Manager, and extensive knowledge was required of H323 interface with the Avaya.

The BRI interface worked with an Avaya ISND 8510T with limited functionality. The phone could be used for a single phone taking calls, but the placement of calls was being blocked at the phone with “Voice Call Blocked”. When an IVUT was connected to the BRI interface it did not work. After talking with a software/BRI engineer, it was found that there are special packets and functionality that have been added for the Navy that require special loads of the base BRI protocol to work, and add support to the features that are currently expected from the BRI communications terminals.

4.4.4.3 SIPx Server Evaluation

Testing was done against a SIPx server (www.sipfoundry.org) and the results were favorable. The SmartLink Micro worked after configuring it for the new SIP proxy IP address. With these findings, it is important to confirm with the manufacturer of the media gateway it's compatibility with the SIP proxy that will be used in the project, and get any design notes they have for the media gateway and the SIP proxy.

To add to reliability and maintainability the external devices should be SIP-enabled at the start. If that is not possible then they should be interfaced with local session controller hardware, such as the Avaya G700 Gateway (Figure 4-31). The Avaya G700 comes with different interface cards to connect the typical interface found on today's US Navy vessels.

Figure 4-31 Avaya G700 Media Gateway (Front View)

4.4.4.5 Additional Considerations

The last option should be acquiring an external media gateway from a different vendor. This method has several different problems:

1. Vendors: It becomes problematic when each of the vendors point to the other as not supporting the SIP specification. Being in the middle forces you to capture and interpret the network traffic, and to qualify the problem to determine the vendor at fault. This can be done using tools like Wireshark (www.wireshark.org) or GL Communications (www.gl.com) PacketScan. We have found that the logging function on the Avaya S8300 is not adequate to troubleshoot SIP errors.

2. Power: Most media gateways come with some kind of power transformer that needs to be connected to 110 VAC. This is very limiting on a vessel, especially when it comes to location and management of the plugged-in unit. The other method is to create a special cord that connects the media gateway to the ship's power using power transformers and conditioning units.

3. Housing: The media gateways can be located either near the end device that is being converted to SIP, or in the area of the Local session controller. Either way, COTS

media gateways are not designed for the shock and vibration that they will be exposed to on a vessel. They are also not designed for the environment on board a Navy vessel. Large units that support several interfaces are 19-inch rack compatible, but most units are small and have no mounting provisions.

4.4.4.6 Conclusion

The best approach is to use devices that are SIP-based by design. This does not mean that problems will be eliminated, but it removes many of the initial problems that come from the use of an external media gateway. The second direction is to use the media gateway that is part of the local session controller, if they offer it. In this case it is a single vendor and it is packaged for the shock, vibration and environment that the local session controller is designed for. The last direction is use independent media gateways. In some cases, connecting to radios and ear and mouth (E&M) units may require this method of interfacing. In those cases, work with the manufacture of the media gateway up front to make sure it is compatible with the local session controller and the end device. If possible, have that vendor do the integration to the local session controller and end device.

4.4.5 Unified Capabilities Requirements 2008 (UCR2008)

This paragraph was extracted from the *Unified Capabilities Requirements 2008* (*Draft 2*) [ ] *(DISN)*. The subparagraphs included are ***Introduction, Unified Capabilities, Purpose*** and ***Applicability*** (other sections of the *Unified Capabilities Requirements 2008 (Draft 2)* used in other parts of this Technical Report are referenced as required).

Introduction

The purpose of this "Unified Capabilities Requirements 2008 (UCR 2008)" document is to specify the technical requirements for network components and telecommunications devices to be used in the Department of Defense (DoD) networks to provide unified capabilities. The technical specifications defined by UCR 2008 support the policies and requirements established by DoD Instruction (DoDI) 8100.3 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C as well as references listed in UCR 2008, Section 3, Policy. UCR 2008 may be used to support acquisition, testing, network management, configuration management, and policy development processes. UCR 2008 identifies only the MINIMUM requirements and features applicable to the overall DoD community. UCR 2008 may not contain a complete set of specifications for the commercial off-the-shelf (COTS) commercial telecommunications devices used to meet these requirements. Procuring agencies may need to include other specifications or additions to have a complete product specification.

Unified Capabilities

Unified capabilities are defined as the seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet

Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities.

Unified capabilities integrate standards-based communication and collaboration services including, but not limited to, the following:

- *Messaging*
- *Voice, video, and Web conferencing*
- *Presence*
- *Unified capabilities clients*

These standards-based communication and collaboration services must integrate with available enterprise applications, both business and warfighting.
UCR 2008 specifies technical requirements for DoD networks and components that support and interact with IP-based real time services (RTS), which are used to provide the following unified capabilities:

Purpose

- *Telephony. Including soft IP telephony, Internet telephony, and wireless telephony.*
- *Unified Messaging. Integrates voice mail and e-mail.*
- *E-Mail/Calendaring. Represents the way e-mail typically is delivered.*
- *Unified Conferencing. Audio, Web, or videoconferencing integrated into a single, consolidated solution.*
- *Audio Conferencing. Delivered separately as audio conferencing.*
- *Web Conferencing and Web Collaboration. Delivered separately as Web conferencing.*
- *Videoconferencing. Delivered separately as videoconferencing.*
- *Mobility. Provides the ability to offer wireless access and applies to telephony, e-mail, and many other communication applications. It includes devices such as personal digital assistants (PDAs) and smart phones. In addition, it considers how solutions integrate on-premise enterprise functions with the functions of mobile operators.*

Applicability

UCR 2008 applicability is defined based on CJCSI 6215.01C, as follows:
"3. Applicability. This instruction applies to Office of the Secretary of Defense, the Military Services, Chairman of the Joint Chiefs of Staff, combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DOD Field Activities and all other organizational entities in the Department of Defense (referred to hereafter collectively as "the DOD components") in peacetime, crisis situations, and wartime. This instruction also identifies policy and responsibilities concerning non-DOD governmental, foreign government, and civilian organizational

requests for DSN, DRSN, and DISN Assured RTS support (DARTS). Requests for waivers this instruction will be forwarded through the DOD component chain of command to the Joint Staff, stating the reason compliance is not possible. This instruction is applicable to:

> *"a. All telecommunications switches leased, procured (whether systems or services), or operated by any DOD component of the Department of Defense.*
> *"b. The hardware or software for sending and receiving voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the DSN, DRSN or public switched telephone networks (PSTN).*
> *"c. End-to-End services (e.g., phone-to-phone, video-to-video units, fax-to-fax; secure terminal equipment (STE-to-STE) to include tactical applications.*
> *"d. All technologies i.e. (circuit switch, voice over Asynchronous Transfer Mode (ATM), and Voice over Internet Protocol (VoIP)) that use DSN or DRSN phone numbers; or that are otherwise incorporated into the DSN or DRSN numbering or routing plans via area code, access code, Internet Protocol (IP) addressing scheme, etc. for the origination and reception of voice, dial-up video, and dial-up data for routine and precedence subscribers.*
> *"e. The DOD component's planning, investment, development, operations, and management of telecommunications switches connected to the DSN or DRSN for processing voice, dial-up video and dial-up data.*
> *"f. All networks that provide DISN RTS."*

This specification applies to all network components and telecommunications devices to be used in DoD networks that provide the unified capabilities defined in UCR 2008, Section 1.2, Unified Capabilities. All services, features, and functions (i.e., military unique, assured, and standard commercial) identified in UCR 2008 are to be implemented in all network assets including TDMbased equipment (e.g., Multifunction Switch (MFS), End Office (EO), Small End Office (SMEO), Private Branch Exchange Type 1 (PBX1) and Type 2 (PBX2), Deployable Voice Exchange (DVX), secure telephones, Integrated Services Digital Network (ISDN) video) as defined in CJCSI 6215.01C and IP-based equipment (e.g., Local Session Controller (LSC), Edge Boundary Controller (EBC), Customer Edge Router (CER), Assured Services Local Area Network (ASLAN), Wide Area Network (WAN), Assured Services Session Initiation Protocol (AS-SIP) used as signaling within the IP environment, Customer Premises Equipment (CPE), and ancillary equipment). See Appendix A, Definitions, Abbreviations and Acronyms, and References, for more details. In addition, this specification applies to upgrades and new software loads for existing equipment.

UCR 2008 is the governing specification document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of UCR 2008 take precedence over the explicit or implicit requirements of the Local Access and Transport Area (LATA) Switching Systems Generic Requirements (LSSGR) and Internet Engineering Task Force (IETF) Requests for Comment (RFCs).

4.4.6 Conclusion

The CANES program covers the Integrated Shipboard Network System by outlining equipment requirements and bringing together different networks into a single consistently managed network with the same hardware. The UCR2008 covers the reliability of the underlying structure and the top level protocols. This, incorporated with the Security Technical Implementation Guidelines (STIG), will establish requirements to secure and make the whole network and the functions that run on top of it more reliable. The media gateway manufacturer needs to be consulted to determine if compatibility testing has been done with the media gateway and the SIP proxy that will be used in the network. The recommendation is to avoid the use of a media gateway if possible, but if not, then using one that is incorporated into the local session controller is the best approach. The use of an external media gateway should be avoided if possible but in some cases it cannot be. In those cases, work closely with the manufacturer of the media gateway to confirm compatibility with the local session controller as well as the end device. In most cases this would be limited to special devices like radios and E&M devices like Sound-Powered Telephones (SPT).

If the network is designed up-front as CANES describes and layered with the UCR, the network becomes more maintainable. Even so, the interface to the network needs to allow the individual sailor without a Master’s Degree in Computer Science to be able to manage it. This has been a major effort at Boeing’s dual-redundant mesh network, which has created a single management point that tells the user in plain English the complete state of the system, and allows the user to troubleshoot any switch and make changes. Implementation of the above will allow for a reliable and maintainable VoIP system, as well as other systems in the vessel.

4.5 Feasibility of IP-Announcing

4.5.1 Introduction

Announcing is a critical internal communications method. Announcing is used for general announcements, but also for distribution of critical information. The flight deck of an aircraft carrier is a major user of announcing and it is a challenging environment for any kind of audio broadcast.

IP Announcing means using the IP network infrastructure to carry the announcements instead of dedicated cable runs. However, there are many benefits to dedicated cable runs that should not be overlooked. The main benefit is that separate power is not required to each of the speakers; the cable itself carries the analog signal and the power to drive the speaker. The traditional design's cables are connected to a group of amplifiers that supply the power and signal, but there is a dedicated cable per each speaker. This design has been implemented on almost every large vessel, as well as smaller and submerged vessels in the fleet.

IP Announcing is very different in its topology in that it is more distributed in nature. The amplifiers are built into the speakers requiring power. This can be either through Power over Ethernet (PoE) or ships power depending on the wattage required for the particular speaker location. In many cases, distributed architecture with the use of PoE allows for a reduction of heavy wire and power can be supplied locally, not from the amplifiers cabinet. The PoE comes from the last network switch in the topology, so a single or redundant wire or fiber can be used to transport the audio stream from the announcing server to the edge switch, and then the last length of cable to the speaker carries the power for the speaker.

A hybrid design combining the two technologies may be the ultimate solution. The use of distributed power amplifiers and IP-based speakers may reduce the wiring requirements, and result in the level of performance that is required for this critical form of communications.

4.5.1.1 IP Announcing and Commercial-Off-the-Shelf (COTS) Systems

There have been several vendors that have moved into the commercial IP Announcing marketplace. The different systems all have different features, but all of them meet the requirements for announcing in a commercial environment. The announcing servers are feature rich in many ways, but very limited in others. The standard process starts with a tone; after the user enters the zone number and then another tone, the user can make the announcement. The tones alienate the user so the announcement is not cut off. It is a slow process compared to the current design, which allows the user to press a button on a microphone station and make an announcement. Commercial systems have two types of speaker configurations:

1. Session Initiation Protocol (SIP) Based – This configuration requires that each speaker log into the SIP server as an extension on the switch. This has the benefit of each speaker being reached directly by dialing its extension, hearing the tone, and then making announcements to the single speaker. Conference groups can be created and multiple speakers included in the group and announcements made through all. Another benefit is inclusion of IP phones that support “auto answer” in the conference group. This type of announcing is supported in some types of open source PBX like sipX by SIPfoundry. (http://www.sipfoundry.org/sipX).

2. Multicast Based – In this configuration, the speakers listen to a set IP address and port for the announcement. Large groups of speakers can be handled directly from the announcing server. In this solution the IP PBX only has to support a single extension for the page server. However, this configuration is limited by not allowing phones to be included in the page or accessing the speakers directly by an extension.

The current commercial announcing server, with its requirement to enter a zone number and the time for the two-digit tones, limits its ability to be used for quick and automatic announcements. Page servers and speakers are not designed for the shock, vibration, and environmental conditions required for shipboard use. The software design would need to have discrete inputs so the zones could be entered from the microphone station instead of entered during the paging process.

Figure 4-32 is an illustration of a COTS Announcing System that contains many of the following typical requirements:

- Analog Phone – can access the page server through a media gateway that is contained within the Avaya PBX.
- IP Speakers PoE Powered – speakers are powered from the Ethernet cable that carries the IP packets. The power is supplied from the last network switch and it requires copper to the speaker to carry the required power.
- IP Speaker External Power – this speaker gets the announcement over the IP network but the power is supplied externally from ships power.
- IP PBX – handles the calls and directs them to the page server.
- Network Switch – this switch connects the different components to each other, as well as supplying power to the devices that require it.
- IP Phone – this phone connects to the IP PBX and accesses the page server to initiate the announcement.
- Page Server – this component takes in the call and selects the zone (group of speakers) and broadcasts the announcement over the speakers.
- Amplifier – this is the current type of amplifier that is used but implemented with an IP interface to get its announcements from the page server and not an audio input, as it would in a traditional system.

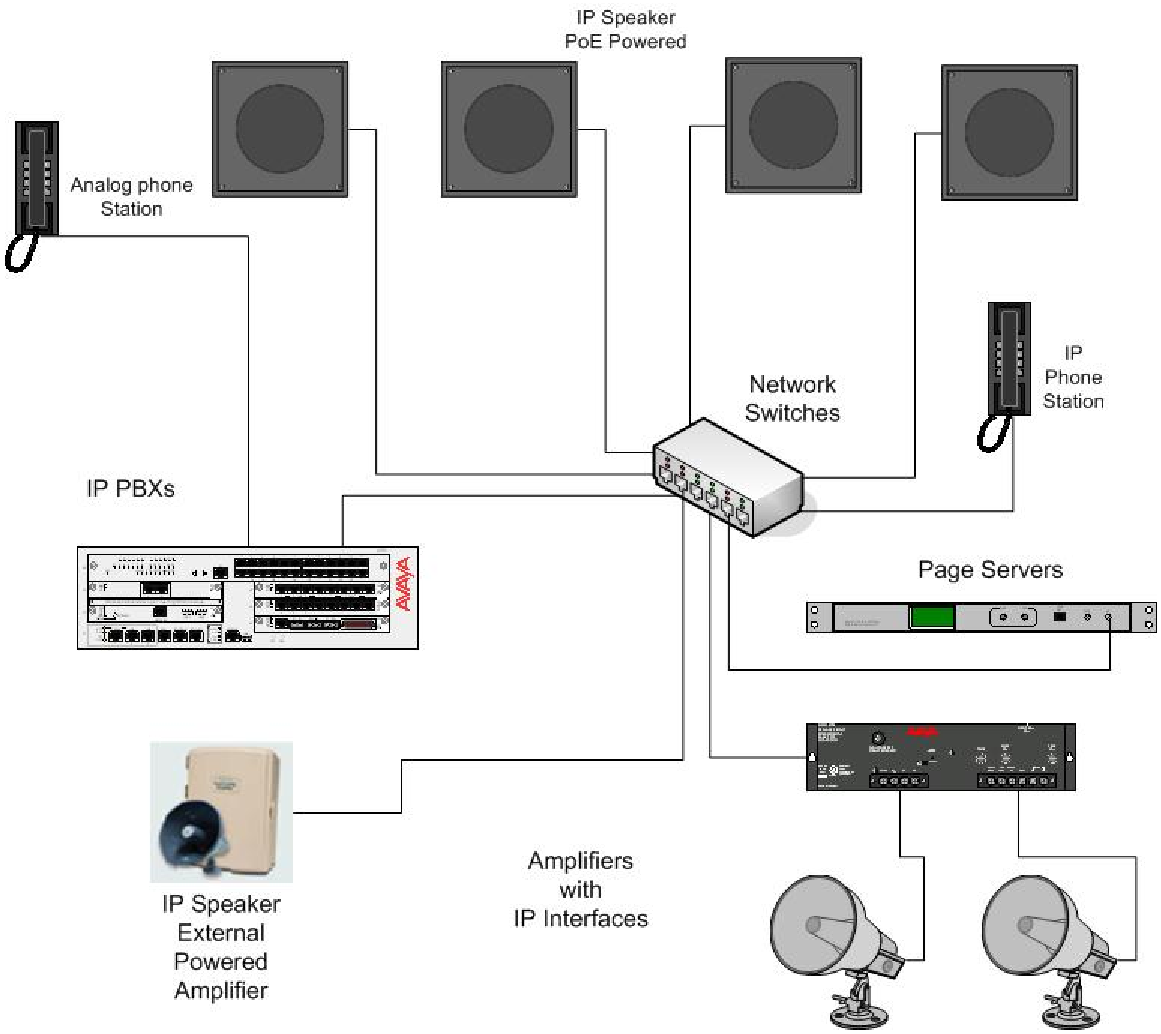


Figure 4-32 COTS Announcing System

The zone configuration is setup in the page server as well as the speakers. The speakers are configured to monitor defined multicast addresses and ports. The page server is then configured with the different zones, and the priority set for the individual zones. The resulting matrix is represented in Table 4-8:

Table 4-8 Zone Configuration

	Speakers			
Zones	81	82	83	84
1		X	X	
2				X
3				
4	X	X	X	

Table 4-8 Zone Configuration – Continued

	Speakers			
Zones	81	82	83	84
5				X
6	X	X		X
7			X	
8	X	X	X	X
9 (Note 1)	X	X	X	X
10 (Note 2)	X	X	X	X

Note 1: Zone 9 is a high priority zone that all speakers are included in, so any page to that zone would be heard on all speakers.

Note 2: Zone 10 is a background zone so all other announcements are heard over its announcement. In commercial use, this zone could have background music, but be pre-empted by any other zone.

4.5.1.2 Latency and IP Announcing

One concern that has been heard from many different sources is the current latency experienced in areas like the hanger bays of an aircraft carrier. This is an area that will need to be tested to determine if it can be improved by IP, or at least maintain the current latency issues. In the optimal design, the speakers would be mounted off of a single switch or a set of switches that have been ganged together and used for announcing only. The use of fiber instead of wire would also help resolve the latency problem. With this design, there would be no network traffic on the connections from the switch to create jitter or latency. Another approach would be to bring the audio stream to the location via IP, and then connect the speakers to a power amplifier. The latency is then controlled by the length of wire between the amplifiers and the speakers.

4.5.1.3 Hybrid Announcing Design

A design that is a hybrid of both the central amplifier and IP speakers could be a very clean solution. The amplifiers require long runs of wire unless they are closer to the required system location. IP could be used to connect to the individual amplifiers and reduce the overall weight of the installation. If fiber is used for the connection, even more weight is reduced and high data rates can be achieved. The fiber can also be passed through critical areas that require copper to use specialized shielding. In areas like berthing, PoE speakers could be used that do not require the same db levels as nosier locations. In the design shown in Figure 4-32, there is redundancy between speakers and major components. The current COTS amplifiers are not redundant, this is value-added that puts the Announcing System into a cabinet as it is packaged for the vessel. IP announcing from COTS suppliers do not have redundancy.

Figure 4-33 is an illustration of a hybrid announcing system that contains many of the following typical requirements:

- Analog Phone – can access the page server through a media gateway that is contained within the Avaya PBX
- IP Speakers PoE Powered – speakers are powered from the Ethernet cable that carries the IP packets. Power is supplied from the last network switch which requires copper to the speaker. These speakers are dual-homed so the IP path and power is supplied by two separate switches, which means either switch could fail and the speakers would continue to work.
- IP PBX – used to handle the calls and direct them to the page server. In this design, a high availability configuration is shown.
- Network Switch – the switch connects the different components to each other as well as supplying power to the devices that require it. In a fully redundant network, there would be a partial meshed or Gigabit Ethernet Data Multiplex System (GEDMS) network that is represented by the two switches shown in Figure 3-2.
- IP Phone – connects to the IP PBX and can access the page server to initiate the announcement.
- Page Server – takes in the call and selects the zone (group of speakers) and broadcasts the announcement over the speakers. The page server would have to be developed to support high availability.
- Amplifier – This is the current type of amplifier that is used but implemented with an IP interface to get announcements from the page server and not an audio input, as would be done in a traditional system. The IP interfaces for the amplifiers would also need to be designed to support high availability.

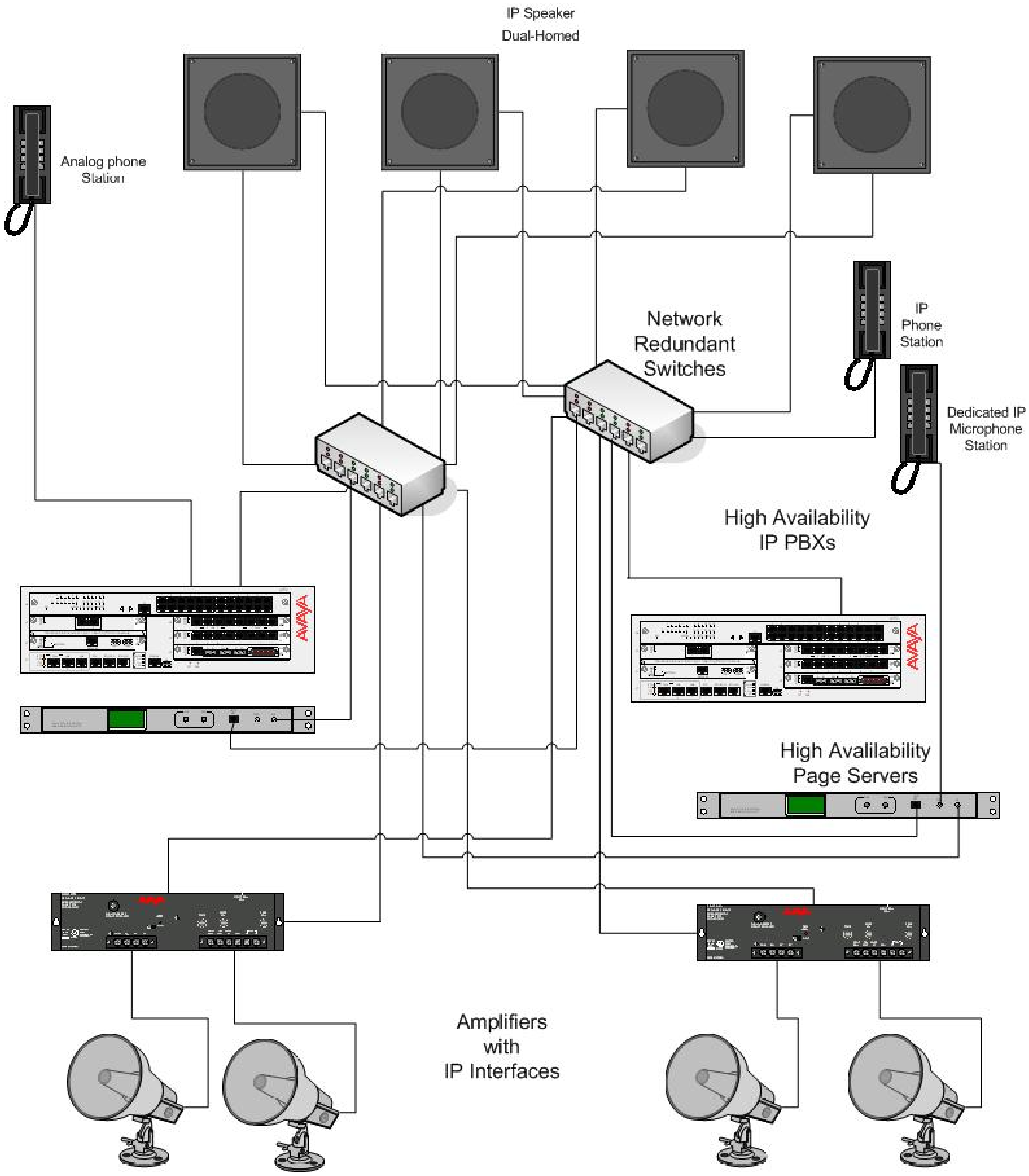


Figure 4-33 Hybrid Announcing System

4.5.2 IP Announcing Shortcomings

The COTS products that are currently available today are non-redundant and do not support any type of high availability scheme. The speakers would need to be developed with dual-homed network connections that would then be routed through different edge

and core network switches. The page server would also need to be designed as high-availability or redundant - either design method will need to have a fail-over to another unit located in a different part of the vessel.

The current offering network connections are copper only. The introduction of fiber would allow for the systems to be connected to fast ports and reduce the weight of copper runs. Fiber has many other qualities on board a vessel. However, the end run to the speakers still needs to be copper to support the PoE of low-wattage speakers.

The IP Announcing system would need to be closely integrated with the IP PBX and the network resources to reduce the possibility of failure. The speakers would need to be dual-homed and connect to the same multicast socket that determines which packet they will use for the announcement; this type of configuration has been done with the navigational packets for many years. The speakers would need to know the master page server and then slave and monitor them both. This type of high-availability has been implemented into several COTs IP PBX systems, as well as some of the open source ones like SIPx from SIPfoundry.org.

4.5.3 Conclusion

The Hybrid Announcing System brings to the naval vessel the best of both technologies. The IP sections let the system reduce wire pulls because a single network fiber or dual-fiber can be connected to outer switches that result in reduced wiring requirements. The fiber can already be made available for the backbone network. The amplifiers fulfill the need for areas where the power of a central amplifier is required.

A detailed design needs to be created that utilizes many of the points that have been discussed above and includes them into the design. CyberData Inc., was interested in working with a company to create a line that would fulfill the requirements of the US Navy in redundancy, vibration, shock, and isolations. The hybrid design shown in Figure 4-33 is a base for a hybrid system, but many critical points are not covered in the design.

This page intentionally left blank.

CHAPTER 5 RECOMMENDATIONS AND CONCLUSION

5.1 Introduction

The technology is ready for final testing and implementation, but tactical requirements dictate that the implementation is carried out as a structured introduction to the Fleet. This structured introduction should also have a backup method that is unwavering in its reliability. The current stable technology is Basic Rate Interchange (BRI) for the US Navy. A hybrid system will allow for testing of the unified voice, data and video, and will allow tactical information to be maintained on the BRI. Initially, administrative communications can be done with VoIP and then expanded outward as it proves its reliability and stability (the new switches from companies like Avaya support both BRI and VoIP). In the next release of the UCR, the end-device support for AS-SIP will be added to the current specification which at this time only supports AS-SIP between local area controllers. VoIP may be the choice for external communications, leaving only on-vessel tactical communications supported by BRI.

5.1.1 Recommendation

To achieve this hybrid solution, L-3 Henschel will continue its research with Phase 3 funding that will build on the knowledge gained in Phase 1 and Phase 2 and expand on it with two related tasks. The first task will expand on the Proof-of-Concept that was developed in Phase 2 and support it in an Assured-Services lab. The second task will expand the Proof-of-Concept into a hybrid design that supports AS-SIP as well as BRI telephony. Testing will gather the results and where possible make changes to the Phase 2 Proof-of -Concept and its environment to extend its functionality. It will also take the information gathered and roll it into the Proof-of-Concept hybrid, expanding on the design and making the unit ready for more intensive testing at a US Navy Lab.

The Proof-of-Concept will prove the ability of AS-SIP to be used on-board a US Navy vessel. It will be designed to exercise the telephony functionalities that are required of an IP Communications Terminal. Its focus will be to test telephony functionality, and the Graphical User Interface (GUI) designs. The design will continue to be done with Telesoft International, Inc (Telesoft) stacks and Global IP Sound (GIPS) voice engine. These third party software products will reduce the time of development since they will be the core telephony and media stream components. This will allow any company to implement the same source code by purchasing rights from the individual companies, or add their own technology if desired.

The objective of Phase 3 is to take the information from the Phase 2 testing and Proof-of-Concept and the information compiled in Phase 1, and create a working Proof-of-Concept so that different groups in the US Navy can evaluate the technology of an IP Communications Terminal that is a hybrid with a BRI capability. The deliverable will be

the Proof-of-Concept hybrid, documentation supporting the implementation, and methods of implementing the two technologies to work in unison. The telephony module will combine the two technologies and present them as a single interface to the GUI/Application developers, so they do not need to learn and understand the differences between the underlying technologies. The GUI/Application will represent the features that are necessary for a sailor to test the functions required, to determine if the technology is ready for ship board implementation. This will include but not be limited to speed dials, numeric dial pad, and selection of types of call. It will not expose features that are for ease of configuration or the ability to switch between multiple profiles. Even though other technologies are made available by connection to the network, limited exploration of them will be done during Phase 3 and they will be left to future productization.

5.1.2 Conclusion

The merging of the first two phases and L-3 Henschel internal research, other US Armed Forces research, doctrines, and rapid advancements in technology result in a solution that will fulfill the needs of the Fleet. The release of the final Unified Capability Requirements 2008 and the planned release of the next version with its support for end-device Assured-Services SIP, allows for a complete solution for the US Navy. The hybrid also allows for the transition from older technologies to newer technologies that have, in many cases, been fielded already with the US Army as well as the US Marines. Unified information on the network including communications and critical data will enhance the ability of sailors to meet their responsibilities; and will result as well in the consolidation of devices with which they need to interface. This will also result in reduced training and reduced equipment, thereby reducing space and wiring requirements. While not at their stations, the wireless phones will give the sailor the same comprehensive functionality as a desk phone.

The use of open source and open architecture products will keep the US Navy from being tied to a single vendor because of proprietary products. It will allow multiple vendors and their products to be combined into a unified network that will support voice, data and video. This direction is achievable; it needs to be implemented so that reliability for our sailors is never compromised in any tactical, as well as non-tactical, scenario.

REFERENCES

This page intentionally left blank

.

Aruba Networks – 1344 Crossman Ave, Sunnyvale, CA 94089 P:408.227.4500 www.arubanetworks.com

Ascom (US) Inc. 598 Airport Blvd., Suite 300 Morrisville, NC 27560 P:919.234.2470 www.ascomwireless.com

Border Gateway Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/BGP, February 3, 2009.

Carrier Grade Voice Over IP, Daniel Collins, McGraw-Hill, Companies, Inc. Copyright 2001, ISBN 0-07-136326-2.

Coltun, R.; D. Ferguson, J Moy, A. Lindem (July 2008). "OSPF for IPv6". Internet Engineering Task Force. Retrieved on 2008-07-23.

DeLorenzo, Alfredo, May 23, 2006, www.voip.com, Voice Quality of Service.

"E^3 and Spectrum Wireless Challenges" Interior Communications Voice Symposium December 3, 2009 J. Don Pierce NAVSEA 05W43, james.d.pierce1@navy.mil , http://icvoicesymposium.com/Presentations/Wednesday/6_Wireless Spectrum and E3 Challenges_Don Pierce.pdf

InnerWireless – 1155 Kas Drive Suite 200, Richardson, TX 75081 P: 972.479.9898 www.innerwireless.com

Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy, SRN L3COM/HENSCHEL/TR -- 2007/001.

LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1990), ANSI/IEEE Std 802.1D, IEEE.

LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1998), ANSI/IEEE Std 802.1D, 1998 Edition, Part 3: Media Access Control (MAC) Bridges, IEEE.

LAN/MAN Standards Committee of the IEEE Computer Society, ed. (2004), ANSI/IEEE Std 802.1D - 2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE.

Meru Networks – 894 Ross Drive, Sunnyvale CA 94089 P: 408.215.5300 www.merunetworks.com

Moy, J. (April 1998). "OSPF Version 2". Internet Engineering Task Force. Retrieved on 2007-09-28.

Open Shortest Path First - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/OSPF, February 3, 2009.

Perlman, Radia (1985). "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN". ACM SIGCOMM Computer Communication Review 15 (4): 44–53. doi:10.1145/318951.319004.

Perlman, Radia (2000). Interconnections, Second Edition. USA: Addison-Wesley. ISBN 0-201-63448-1.

Routing Information Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Routing_Information_Protocol, February 3, 2009.

Spanning Tree Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Spanning_tree_protocol, February 3, 2009.

Subnetwork - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Subnet_Mask, February 3, 2009.

The Industrial Ethernet Book, “VoIP Drives Real Time Ethernet”, Issue 5:29.

The Industrial Ethernet Book, “Quality of Service for High Priority Networks”, Issue 41:36.

Transport Layer Security - Wikipedia, the free encyclopedia, Transport Layer Security - Wikipedia, the free encyclopedia, January 30, 2009.

Understanding Voice Files, GL Communications Inc.

"Understanding Rapid Spanning Tree Protocol (802.1w)". http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml. Retrieved on 2008-11-27.

“Universal Wireless Infrastructure Structure” MobileAccess Networks Interior Communications Voice Symposium December 3, 2009 http://icvoicesymposium.com/Presentations/Wednesday/10_Universal

Voice Quality Testing Reference Document (PSQM, PAMS, PESQ LQ/LQO/WB), GL Communications Inc., June 2008.

VoIP User, SIP and NAT - An Introduction, October 05, 2006.

Waldemar Wojdak (March 2003 [CPCI203]). "Rapid Spanning Tree Protocol: A new solution from an old technology". http://www.compactpci-systems.com/articles/id/?203. Retrieved on 2008-08-04.

Webopedia, SSL definition, http://www.webopedia.com/TERM/S/SSL.html

Wireless Infrastructure_MobileAccess Networks.pdf
Mobile Access Networks – 8391 Old Courthouse Road, Vienna, VA P: 866.431.9266
www.mobileaccessnetworks.com

This page intentionally left blank.

APPENDIX A

iACT MEAN OPINION SCORE PROCEDURES

This page intentionally left blank.

A.1 Test Setup

Figure A-1 shows the setup used for evaluating iACT.

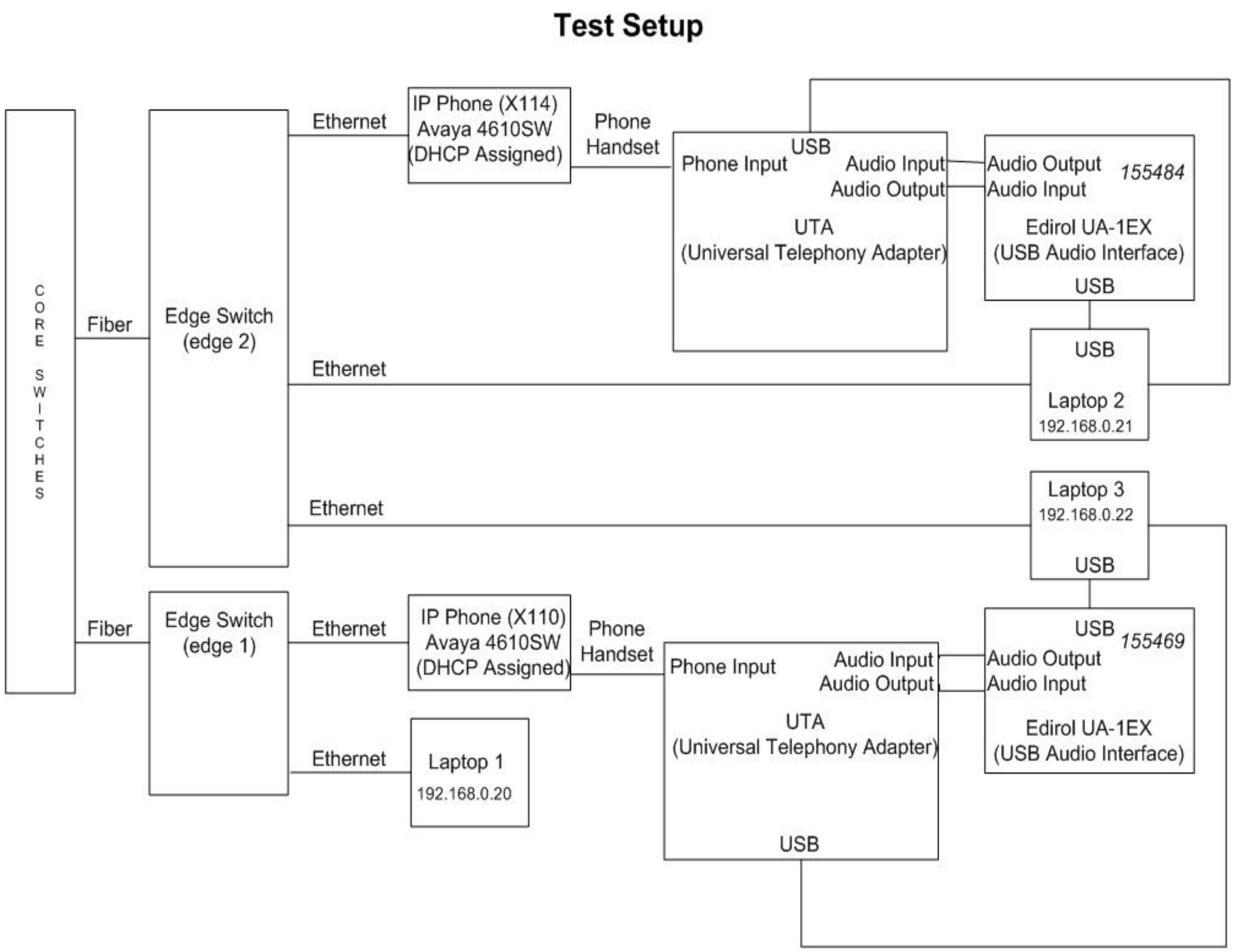


Figure A-1 Test Setup

A.2 Calibration

The audio signals are calibrated to assure that they are starting at the same baseline level before testing is performed in order to assure we have a consistent base to work from.

A.2.1 Initial State

In the initial state of the system, the following will be observed:

1) The system is configured as shown in
2) Figure A-1 with the exception that the phones are not connected to their associated UTA.

3) The handsets are connected to their associated phones.
4) The dial tone can be heard in the handset.
5) The handsets are on-hook.

A.2.2 Establish Voice Connection

Perform the following procedure to establish a voice connection between the two IP phones. When this procedure is completed the IP Phones will communicate with each other through the telephony system as shown in Figure A-1.

1) From one of the IP phones (x114 in this example), dial the other IP phone (x110 in this example). The direction of calling does not matter but for argument sake the direction of calling is assumed to be from x114 to x110.
2) Answer the IP phone at x110 and verify that there is a voice connection.
3) Disconnect the phone wire at the handset-end from each of the IP phones.
4) Connect the phone wire (originally connected to the handset) to the Phone jack of the UTA for both IP phones.
5) Assure that the Mobile/Landline switch on the UTA is set to Landline.
6) Assure that the 3-Wire/4-Wire Switch on the UTA is set to 4-wire.

A.2.3 Calibrate Audio Signals

Perform the following procedure to calibrate the Audio signals between the IP phones. The signal level will be adjusted to between -10dB and -20dB with -15dB being the nominal value.

1) Run the VQuad program on Laptops 2 & 3 by double clicking on the desktop shortcut 

.

2) The VQuad window on Laptop 2 will appear as shown in Figure A-2.

3) A similar window will appear on Laptop 3 with the exception that ***mobile 1*** will be ***mobile 2*** on Laptop 3.

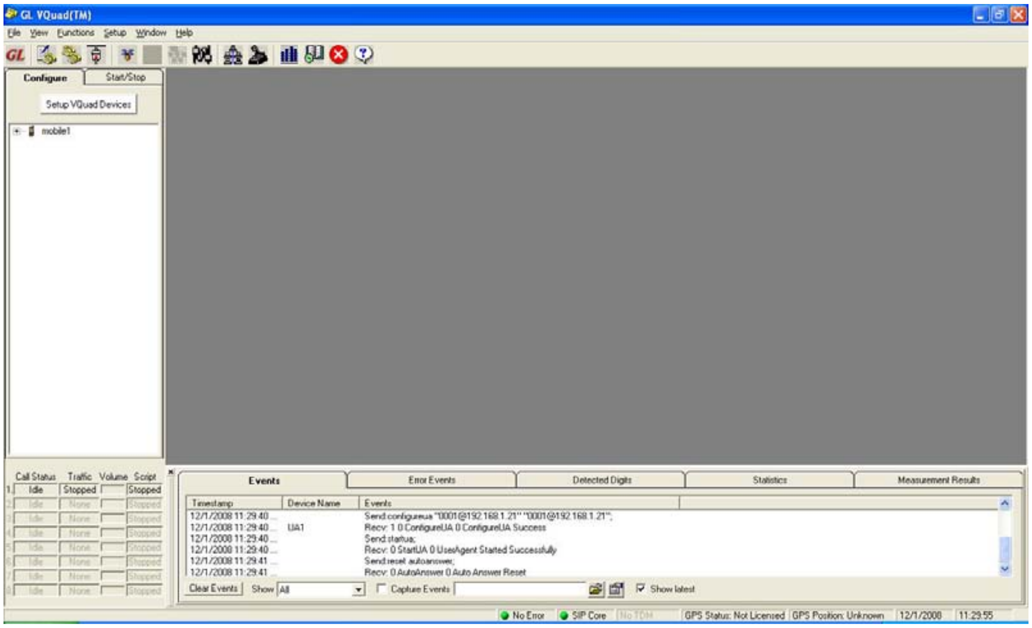


Figure A-2 VQuad Main Window

Verify that the UTA's are associated with the appropriate laptops. To do this, click on the Device Association button  in the VQuad window. The window shown in Figure A-3 will appear.

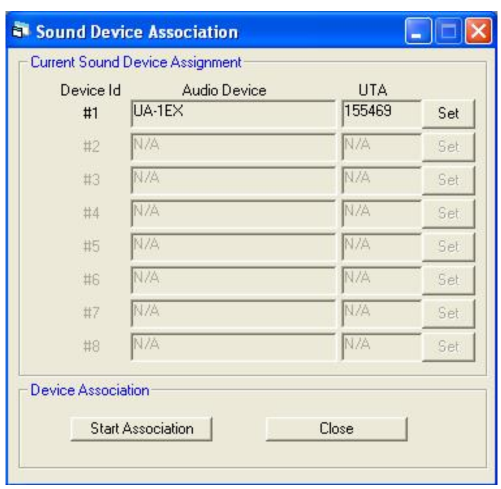
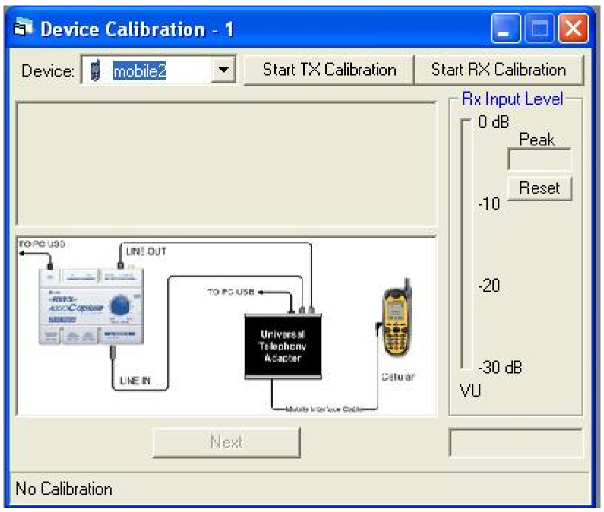


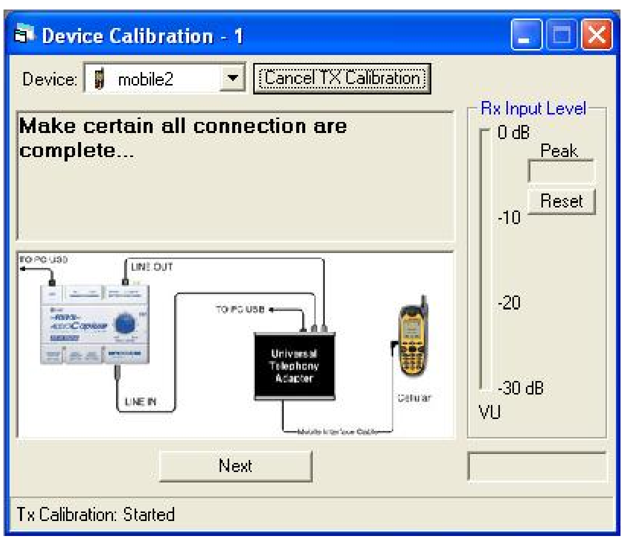
Figure A-3 Sound Device Association Window (Laptop 3)

1) Verify that the S/N found on the bottom of the UTA (and also shown in Figure A-3) matches that which is listed in the ***UTA*** text box. Perform this on both Laptops.

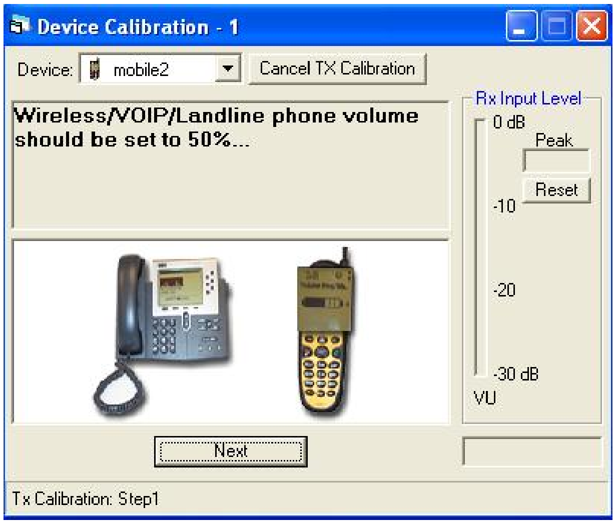
2) Click on the ***Close*** button.
3) In the VQuad window on both laptops, click on the Device Calibration button .
4) Close the ***Device Calibration – 2*** windows on both laptops.
5) On Laptop 3, perform the following steps:



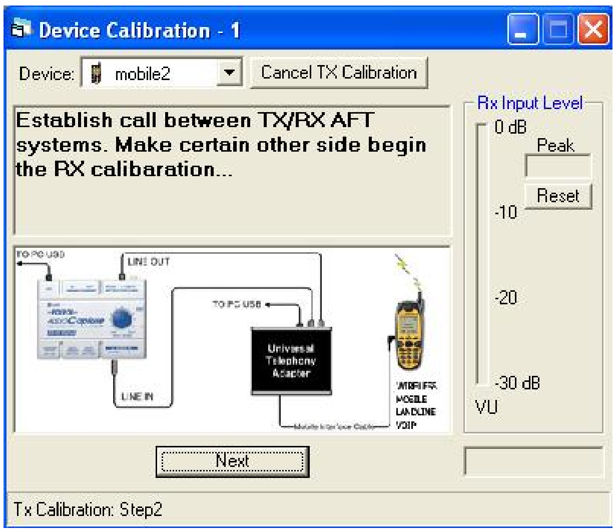
a) Click on the Start TX Calibration button.



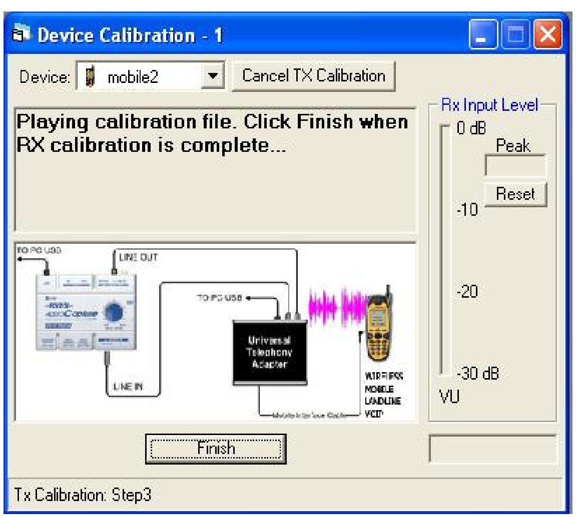
b) Click on the Next button.



c) Click on the Next button.

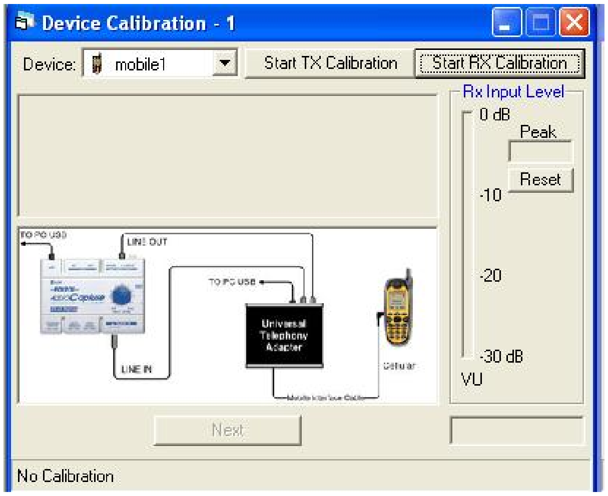


d) Click on the Next button.

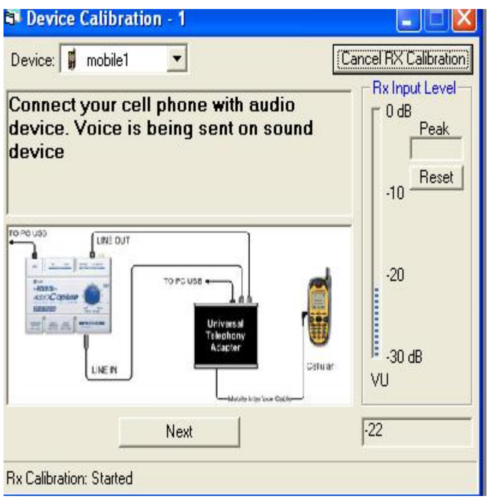


e) Leave this screen up and go to Laptop 2.

6) On Laptop 2, perform the following steps:

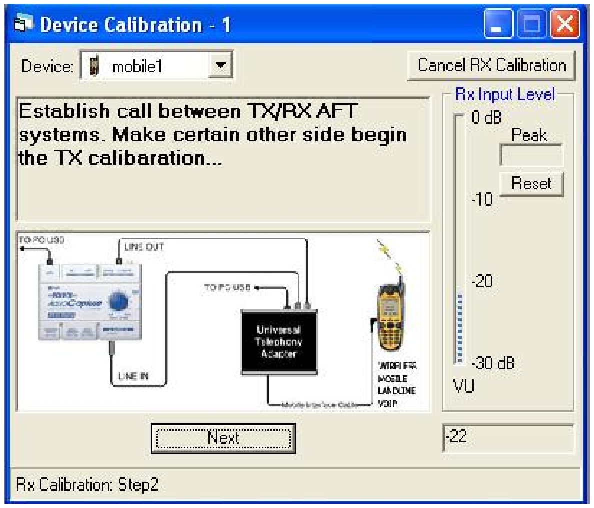


a) Click on the Start RX Calibration button.



b) Click on the Next button.

c) Click on the Next button.



d) Click on the Next button.

e) At this point you should see an Audio signal strength indication in the ***"RX Input Level"*** gauge. This will fluctuate with the maximum signal strength being recorded in the ***Peak*** text box. Adjust either the phone volume (on x114), the Phone Volume adjustment on the USB Adapter Interface, or both until the Peak value recorded is -15dB. Start with the two phones at 50% volume. Try to keep both adjustments from being set to 100%.

7) After calibration is achieved, click on the Finish button in the Calibration window on both laptops.
8) Repeat steps 4 – 6 above reversing the roles of each laptop. Step 4 will be done on Laptop 2 and step 5 will be done on Laptop 3. In step 5e the IP phone x110 will control the volume.
9) Close the Device Calibration windows on both Laptops but leave the VQuad program running.
10) Don't hang-up the two handsets.

A.3 MOS (Mean Opinion Score) Evaluation

The MOS value is an indication of the quality of voice information on a scale of 1 to 5 with 5 being perfect and 1 being inaudible. It is a close approximation of the average rating that would be assigned to voice if it were to be evaluated by human listeners (typically 16 or more). Due to human idiosyncrasies (in general people tend not to assign the highest rating to things) and also that no voice reproduction equipment is perfect, the maximum MOS rating tends to be closer to 4.5.

At a high level, the following will occur during the execution of this evaluation:

1) Four reference files (in the "Reference" folder) containing audio data are transmitted over the phones talk path from one laptop to the other by the VQuad program. The reference files used for our evaluation are:
   C:\VQT_Reference\Samples_Wav\fem1.wav
   C:\VQT_Reference\Samples_Wav\fem2.wav
   C:\VQT_Reference\Samples_Wav\male1.wav
   C:\VQT_Reference\Samples_Wav\male2.wav
2) The receiving laptop stores the received voice data in a "Degraded" folder.
3) A second program (FTU – File Transfer Utility) running on Laptop 1 will copy the contents of the "Degraded" folder from Laptops 2 & 3.
4) A third program (VQT – Voice Quality Tester) running on Laptop 1 compares the reference files with the degraded files and calculates the MOS (Mean Opinion Score) value from these files.
5) The VQT program also calculates Jitter and other parametric values which are important to the overall quality of the audio signal.
6) The output of VQT is stored in an MS-Access database. It can also be exported into an MS-Excel spreadsheet where it can then be charted/graphed/analyzed in many different ways.

A.3.1 Voice Transmission/Reception

This paragraph describes how to use the VQuad program to send and receive voice data. The voice data will be used for analysis in a later step. Perform the following steps:

1) Delete all old degraded voice files on Laptops 1 -3. The voice files are located in the following folders: Note: Don't delete the folders.
   C:\VQT_Degraded\1
   C:\VQT_Degraded\2
   C:\VQT_Degraded\4
   C:\VQT_Degraded\5
2) Assure that the clocks on Laptops 2 & 3 are synchronized within a second of each other.
3) Click on the **+** sign next to mobile 1 on Laptop 2 and mobile 2 on Laptop 3 to expand the trees as shown in Figure A-4.

Laptop 2 **Laptop 3**

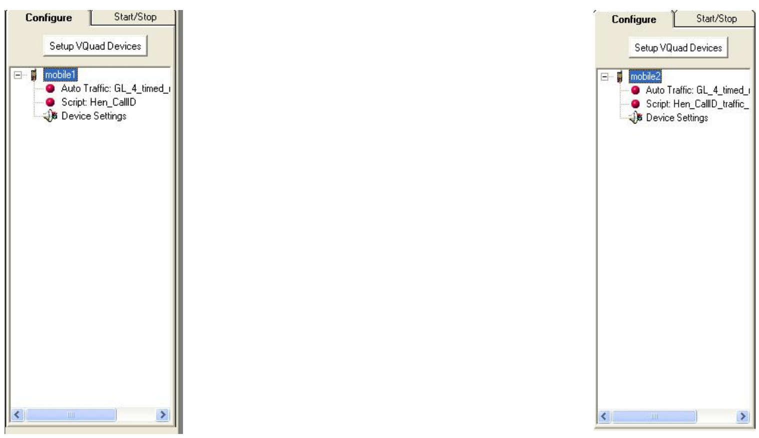


Figure A-4 VQuad Screens

4) Right click on the ***Script: Hen_CallID_traffic_Controler-4-raw*** entry on Laptop 3 and select "edit". In the editor edit the "Create Call ID" for the remote and local and place a name that explains the test to be done. The format should be XXX-YYY-ZZZ where:
   XXX is the connection port into the network (ie: edge1Port2)
   YYY is the name and extension of the device to be tested (ie: PoC114)
   ZZZ is an explanation of the test (ie: Net2VLAN2)
   This will show up in the VQTNetViewer results and will be able to be searched on to query out defined records. Then save the script and close the editor. Then press ***Start Script***. Within a minute the ***Script:***

Hen_CallID_traffic_Controler-4-raw and Auto Traffic: items will change to green on Laptop 3 and the Auto Traffic: item on Laptop 2 will change to Green indicating that the script is running as shown in Figure A-5.

Laptop 2 **Laptop 3**

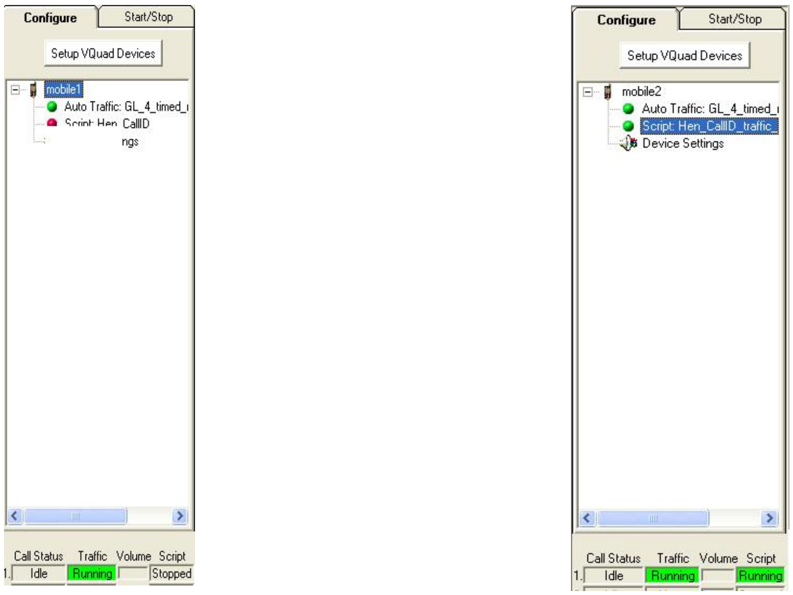


Figure A-5 Running Script Screens

5) Approximately 2 minute after starting the script, files should appear in the following folders on Laptops 2 & 3: (it starts on the next even minute)
   C:\VQT_Degraded\1
   C:\VQT_Degraded\2
   C:\VQT_Degraded\4
   C:\VQT_Degraded\5

A.3.2 FTU (File Transfer Utility)

The purpose of this utility is to copy degraded files from Laptops 2 & 3. The degraded files are being created on both laptops due to the VQuad script which is running. By default the files are copied every 10 seconds (which is configurable) and the degraded files will be deleted automatically from Laptops 2 & 3 once they are copied.

One item of special importance is that the FTU program communicates with a program called ***ASR Listener*** on the laptops. If this program is not running, the file copy will fail on Laptop 1. There should be an Icon for ASR Listener in the System Tray on Laptops 2 & 3. If one doesn't exist, start the ASR Listener program by selecting ***Start→All Programs→ASR Listener***.

Perform the following procedure:

1) On Laptop 1, start the FTU (File Transfer Utility) by double clicking on the desktop shortcut . If the shortcut doesn't exist you can find the FTU program at ***C:\Program Files\GL Communications Inc\VQT\GLFileTransferUtility.exe***. Figure A-6 shows the window that appears.

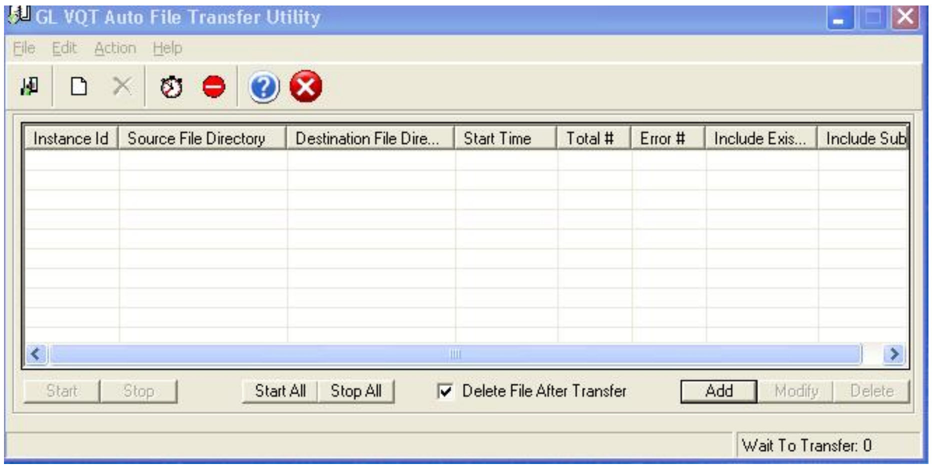


Figure A-6 FTU Program

2) From the FTU tool bar select ***File→Load Configurations***. The window shown in Figure A-7 will appear.

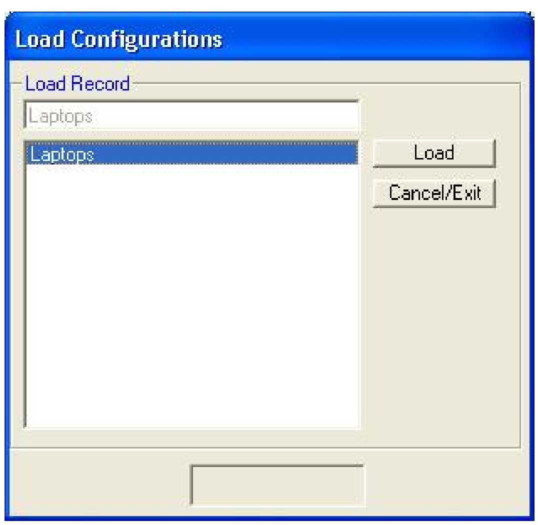


Figure A-7 FTU Load Configurations Window

3) Double click on the ***Laptops*** entry. It will then appear in the ***Load Record*** text box.
4) Click on the ***Load*** button. The window should appear as shown in Figure A-8.

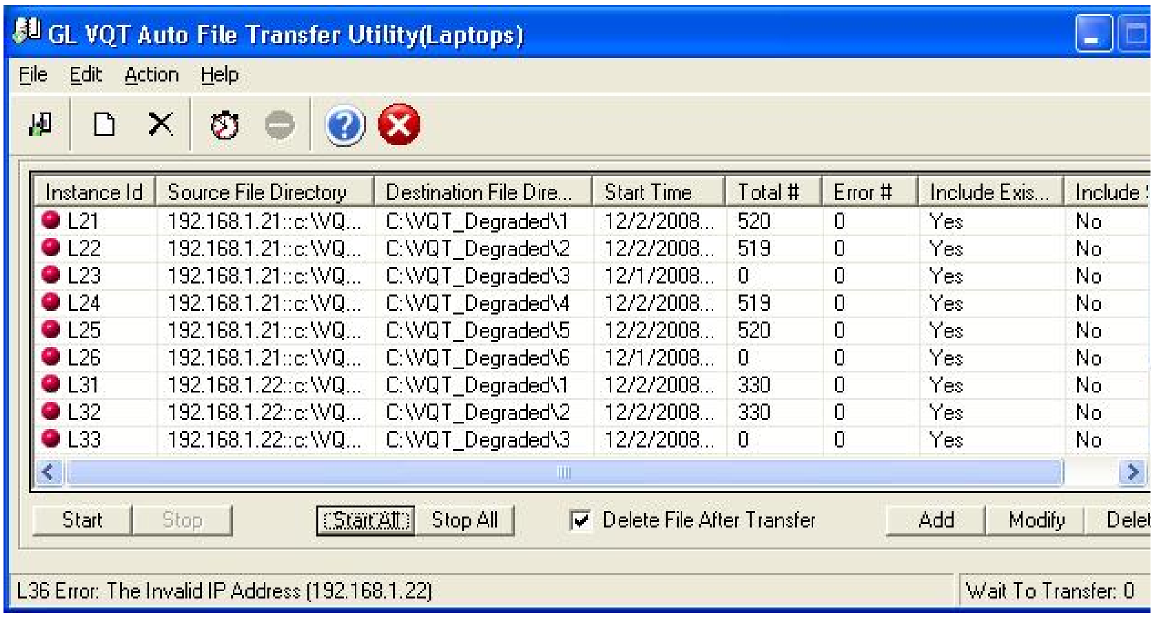


Figure A-8 FTU Window

5) Click on the ***Start All*** button. Each of the items should turn from Red to Green if FTU is able to copy the files. If one or more of the entries does not turn Green, the ASR Listener program may not be running on either Laptop 2, Laptop 3, or both. The window should appear as shown in Figure A-9 (you can tell which laptop by its IP address).

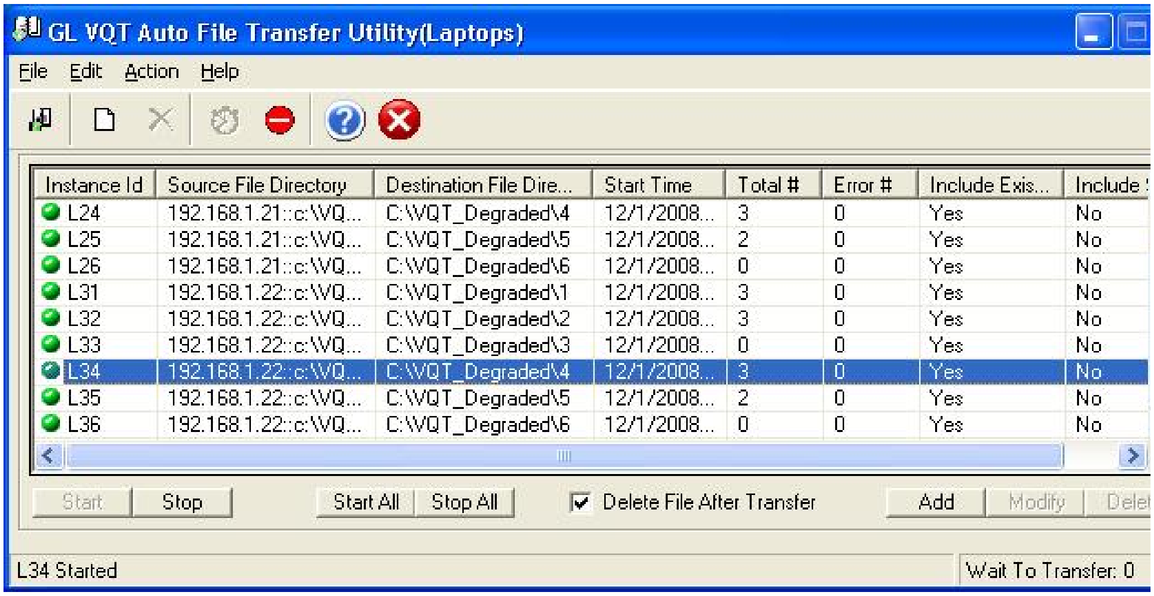


Figure A-9 FTU File Copy Running

6) Verify that files are being copied into the following folders on Laptop 1.

   C:\VQT_Degraded\1
   C:\VQT_Degraded\2
   C:\VQT_Degraded\4
   C:\VQT_Degraded\5

Note 1: These are the only folders which will contain voice files. The other folders listed in Figure A-9 are not used.

Note 2: If you modify the Laptop configuration file (for example to change IP addresses), when saving the new configuration, do not use special characters (i.e. hyphen, underscore, etc…) in the file name.

A.3.3 Data Analysis (VQT)

The purpose of this analysis is to compare the Reference voice files with the Degraded voice files and generate the MOS rating. This is the purpose of the VQT (Voice Quality Tester) program. Perform the following procedure:

1) On Laptop 1, start the VQT (Voice Quality Tester) by double clicking on the desktop shortcut 

. If the shortcut does not exist, you can find the program at ***C:\Program Files\GL Communications Inc\VQT\GL VQT.exe***. The window shown in Figure A-10 will appear.

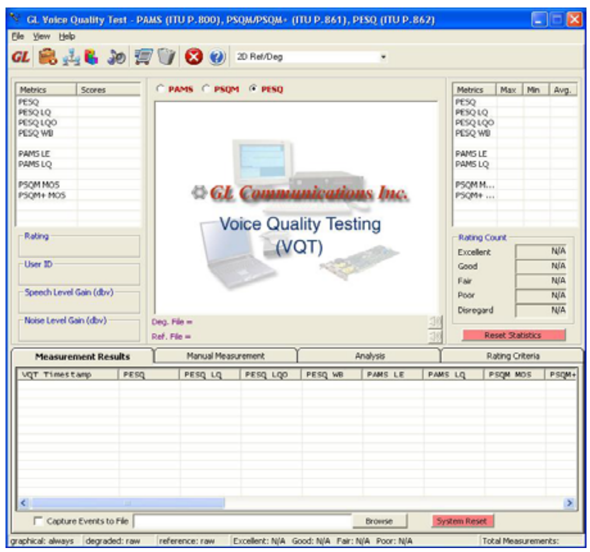


Figure A-10 VQT Window

2) Click on the Auto Measurement button . The window shown in Figure A-11 will appear.

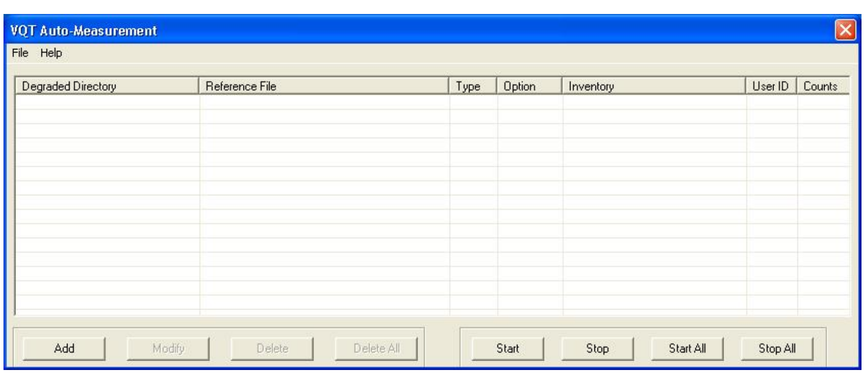


Figure A-11 VQT Auto Measurement Window

3) Select ***File→ Load Auto VQT Configuration*** from the VQT top menu. The window shown in Figure A-12 will appear.

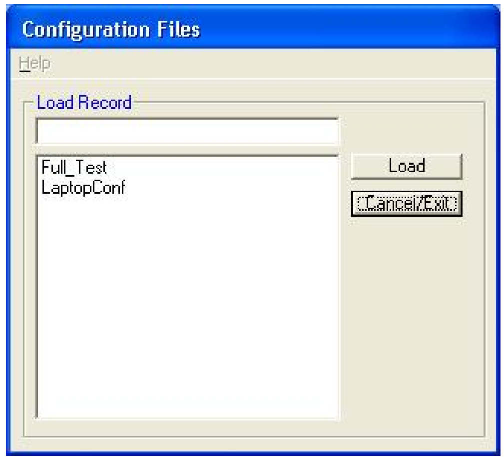


Figure A-12 VQT Configuration Files Screen

4) Double click on ***LaptopConf***. It will appear in the ***Load Record*** text box.

5) Click on the ***Load*** button. The VQT Auto Measurement window will be populated with information concerning the files that VQT will be comparing as shown Figure A-13.

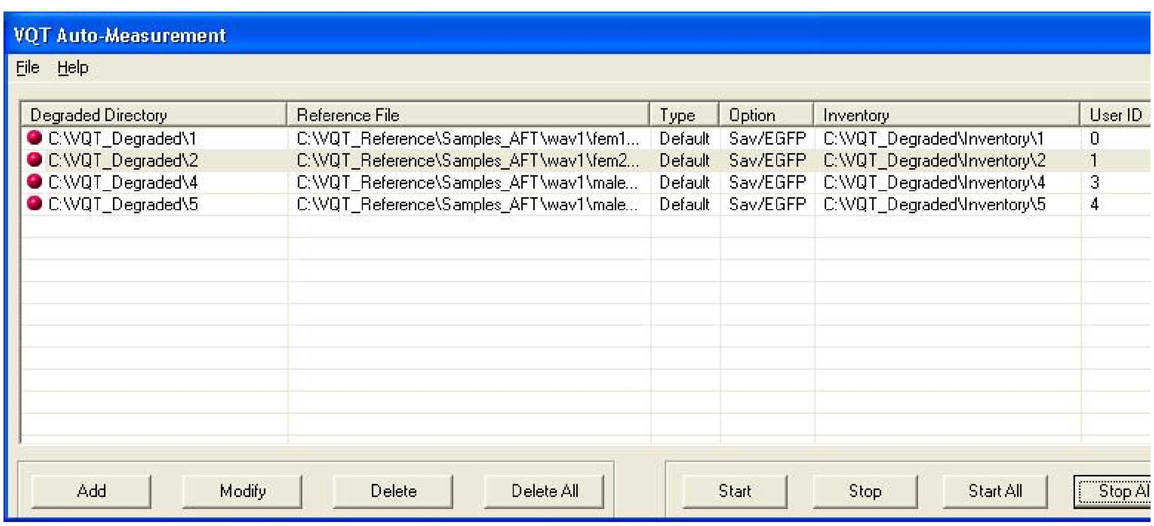


Figure A-13 VQT Auto Measurement Files Window

6) Click on the ***Start All*** button. The entries in the VQT Auto Measurement Files window will change color from Red to Green indicating that the files will be compared by VQT. The VQT window (similar to that shown in Figure A-14) will be populated with values which are the results of VQT's analysis.

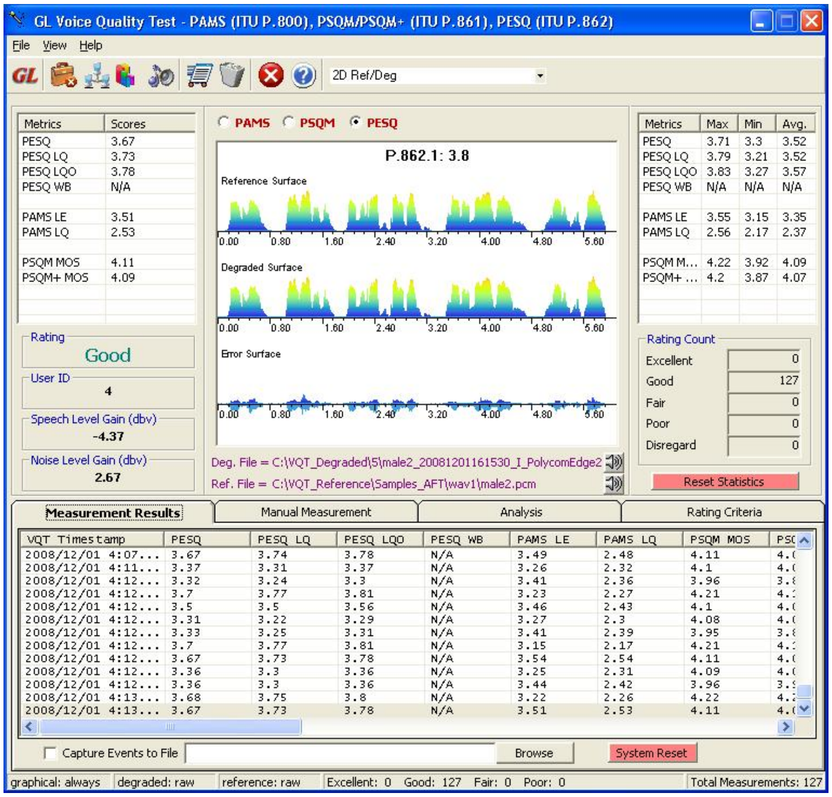


Figure A-14 GL Voice Quality Test Window

7) Verify that the Rating is ***Good*** as indicated in the ***Rating*** text box. VQT is comparing files from four folders. The Reference and Degraded files being compared are shown below the graph. The bottom graph should not deviate much from the baseline.

One problem which may occur during this process is that the files VQT are comparing may be corrupt or incorrectly specified to VQT. Basically, VQT is not comparing the "matched" Reference/Degraded files. In this case it may be quicker to delete all of the degraded files and start this analysis again.

In the VQT Window you may also click on the ***Analysis*** tab to see a different view of the data (Jitter, etc...). This is included here to be informative and is not part of this procedure since we will be analyzing the data through a program called ***VQTNetViewer*** and not through VQT.

A.3.4 Data Viewing (VQTNetViewer)

The purpose of this section is to view the output of the VQT program and to analyze the output to determine the quality of the VoIP system. Perform the following procedure. There is no dongle required for this application.

1) Start the VQTNetViewer program on Laptop 1 by double clicking on the VQTNetViewer desktop shortcut. The program can be run on any of the Laptops but for the sake of argument we'll be using Laptop 1 which is also running the VQT software. The window shown in Figure A-15 will appear.

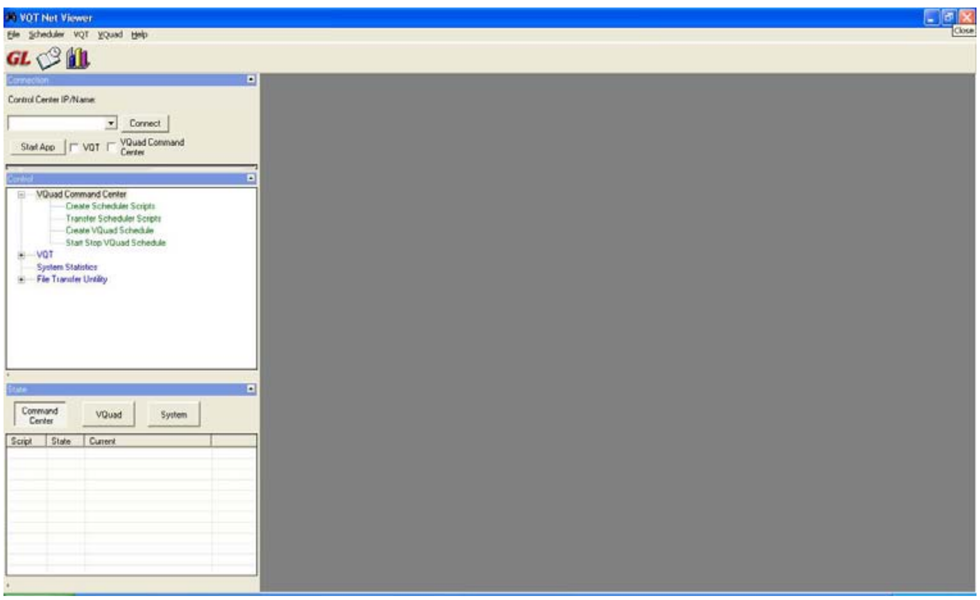


Figure A-15 VQTNetViewer Screen

2) In the ***Control Center IP/Name*** drop-down list box select the IP address of the computer running VQT. This will also be the computer which has the MS-Access database which is being written by VQT. On Laptop 1 the IP address will be shown as 127.0.0.1 which is the "loopback" address. If you are running VQTNetViewer on a Laptop other then Laptop 1, the IP Address will be that of Laptop 1 (192.168.0.20 in our setup).

3) Click on the ***Connect*** button. The window shown in Figure A-16 will appear.

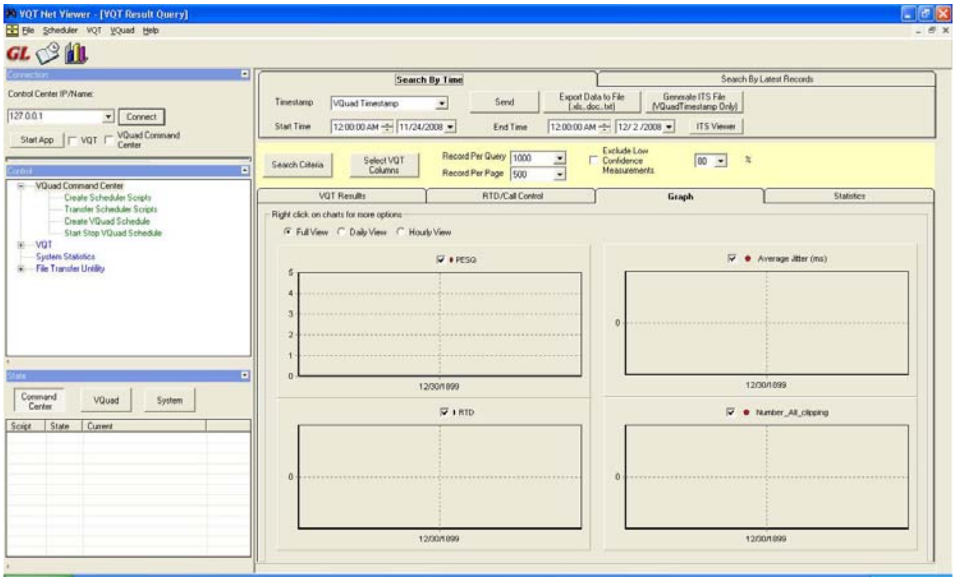


Figure A-16 VQTNetViewer Window

4) Change the ***Start Time*** to when data collection was started. In other words, when the VQT program started to collect data.
5) Change the ***End time*** to the current time.
6) Click on the Send button. This will send an SQL query to the MS-Access database. Data will be plotted on the charts as shown in Figure A-17.

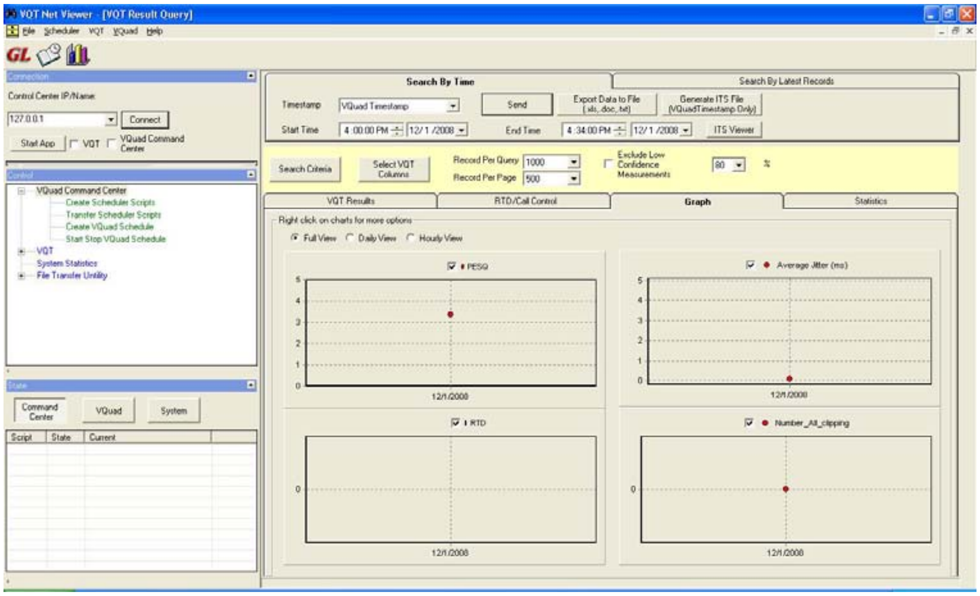
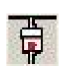


Figure A-17 VQTNetViewer Data Display Window

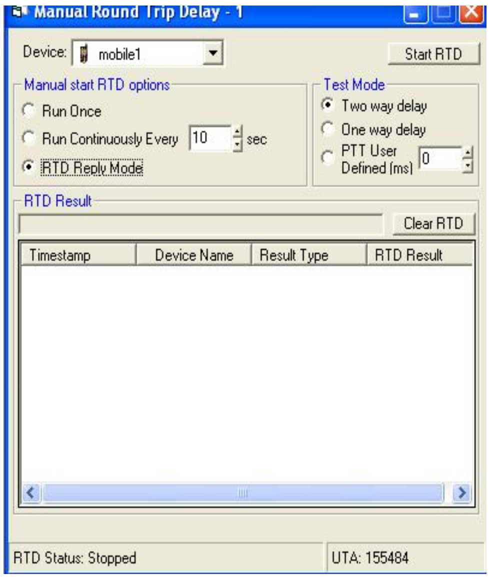
7) Click on the ***Export Data to File*** button.
8) Select a folder and filename to export the MS-Access data to an MS-Excel spreadsheet.

Once the data has been exported to an MS-Excel format it can be read into MS-Excel for final analysis. It is beyond the scope of this document to describe the many ways in which the data can be displayed using MS-Excel. It is assumed that the displaying of the data (MOS Rating, Jitter, etc…) will be customized as appropriate for the feasibility study.

A.4 RTD (Round Trip Delay)

1) Click on the ***RTD*** button  in the ***VQuad*** window on Laptops 2 & 3.
2) Close the ***Manual Round Trip Delay – 2*** windows on both laptops. You will see the windows shown in Figure A-18.

Laptop 2



Laptop 3

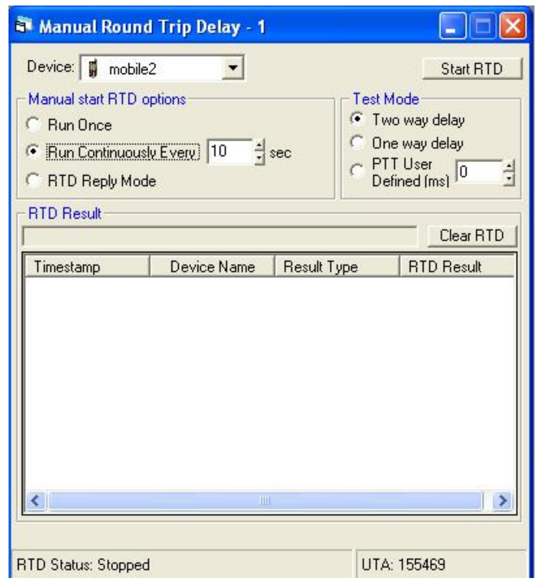
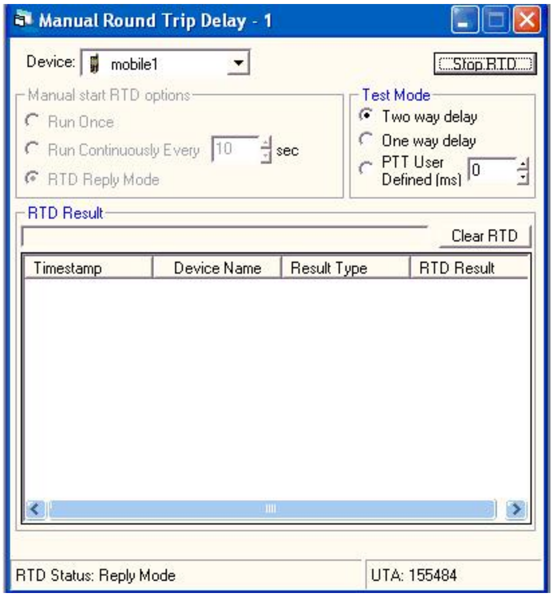


Figure A-18 RTD Main Window

3) Click on the ***RTD Reply Mode*** radio button in the RTD window on Laptop 2.
4) Click on the ***Run Continuously Every*** radio button in the RTD window on Laptop 3.
5) Verify that all other information in the RTD windows are as shown in
6) Figure .
7) Click on the ***Start RTD*** buttons on both laptops. You will see the windows shown in Figure A-19. The data may be different then what is shown but is not expected to be much different.

Laptop 2



Laptop 3

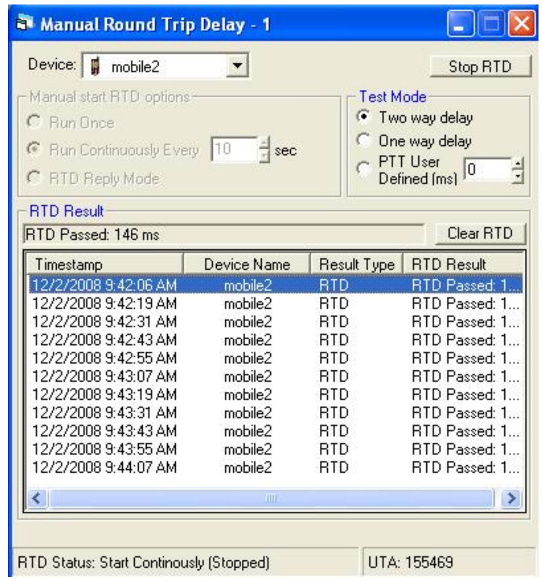


Figure A-19 RTD Running Window

The RTD Result text box contains the amount of time required for the voice file to travel from Laptop 3 to Laptop 2 and back again. The RTD result also includes the time needed to travel through the UTA and USB Adapter.

If the values are negative the volume as setup in paragraph A.2 (calibration) will need to be adjusted. In most cases the volume needs to be reduced to correct the issues. In most cases it is an echo being produced that the sending unit hears and then subtracts the offset of the repeating UTA adds to the process time.

This page intentionally left blank.

APPENDIX B

L3_AS_SIP_Phone INTEROPERABILITY TESTS

This page intentionally left blank.

B.1 L3_AS_SIP_Phone Interoperability Tests

This appendix describes interoperability tests performed using call functions described in Chapter 3, paragraphs 3.2.3.1 thru 3.2.3.6.

> Note: Because the UCR does not (at this time) define the requirements for end devices working with AS-SIP, these tests were used to check the compatibility between devices. The testing was done between PoCs and also with REDCOM devices.

B.1.1 Test 1: Place Outgoing Call Resource Priority Set to Routine

1. Place outgoing call with **routine** resource priority to user on-hook. Observe that call is set up/torn down properly.
2. Place outgoing call with **routine** resource priority to user off-hook with **routine** call. Observe that existing call is not preempted.
3. Place outgoing call with **routine** resource priority to user off-hook with **priority** call. Observe that existing call is not preempted.
4. Place outgoing call with **routine** resource priority to user off-hook with **immediate** call. Observe that existing call is not preempted.
5. Place outgoing call with **routine** resource priority to user off-hook with **flash** call. Observe that existing call is not preempted.
6. Place outgoing call with **routine** resource priority to user off-hook with **flash-override** call. Observe that existing call is not preempted.

B.1.2 Test 2: Place Outgoing Call Resource Priority Set to Priority

1. Place outgoing call with **priority** resource priority to user on-hook. Observe that call is set up/torn down properly.
2. Place outgoing call with **priority** resource priority to user off-hook with **routine** call. Observe that existing call is preempted.
3. Place outgoing call with **priority** resource priority to user off-hook with **priority** call. Observe that existing call is not preempted.
4. Place outgoing call with **priority** resource priority to user off-hook with **immediate** call. Observe that existing call is not preempted.
5. Place outgoing call with **priority** resource priority to user off-hook with **flash** call. Observe that existing call is not preempted.
6. Place outgoing call with **Priority** resource priority to user off-hook with **flash-override** call. Observe that existing call is not preempted.

B.1.3 Test 3: Place Outgoing Call Resource Priority Set to Immediate

1. Place outgoing call with **immediate** resource priority to user on-hook. Observe that call is set up/torn down properly.
2. Place outgoing call with **immediate** resource priority to user off-hook with ‘Routine’ call. Observe that existing call is preempted.
3. Place outgoing call with immediate resource priority to user off-hook with **priority** call. Observe that existing call is preempted.
4. Place outgoing call with **immediate** resource priority to user off-hook with **immediate** call. Observe that existing call is not preempted.
5. Place outgoing call with **immediate** resource priority to user off-hook with **flash** call. Observe that existing call is not preempted.
6. Place outgoing call with **immediate** resource priority to user off-hook with **flash-override** call. Observe that existing call is not preempted.

B.1.4 Test 4: Place Outgoing Call Resource Priority Set to Flash

1. Place outgoing call with **flash** resource priority to user on-hook. Observe that call is set up/torn down properly.
2. Place outgoing call with **flash** resource priority to user off-hook with **routine** call. Observe that existing call is preempted.
3. Place outgoing call with **flash** resource priority to user off-hook with **priority** call. Observe that existing call is preempted.
4. Place outgoing call with **flash** resource priority to user off-hook with **immediate** call. Observe that existing call is preempted.
5. Place outgoing call with **flash** resource priority to user off-hook with **flash** call. Observe that existing call is not preempted.
6. Place outgoing call with **flash** resource priority to user off-hook with **flash-override** call. Observe that existing call is not preempted.

B.1.5 Test 5: Place Outgoing Call Resource Priority Set to Flash-Override

1. Place outgoing call with **flash** resource priority to user on-hook. Observe that call is set up/torn down properly.
2. Place outgoing call with **flash-override** resource priority to user off-hook with **routine** call. Observe that existing call is preempted.
3. Place outgoing call with **flash-override** resource priority to user off-hook with **priority** call. Observe that existing call is preempted.
4. Place outgoing call with **flash-override** resource priority to user off-hook with **immediate** call. Observe that existing call is preempted.

5. Place outgoing call with **flash-override** resource priority to user off-hook with **flash** call. Observe that existing call is preempted.
6. Place outgoing call with **flash-override** resource priority to user off-hook with **flash-override** call. Observe that existing call is not preempted

B.1.6 Test 7: Receive Incoming Call Resource Priority Set to Routine

1. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument not supporting resource priority. Observe that existing call is not preempted.
2. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **routine** to device under test (DUT). Observe that existing call is not preempted.
3. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **priority** to DUT. Observe that existing call is not preempted.
4. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **immediate** to DUT. Observe that existing call is not preempted.
5. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash** to DUT. Observe that existing call is not preempted.
6. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash-override** to DUT. Observe that existing call is not preempted.

B.1.7 Test 8: Receive Incoming Call Resource Priority Set to Priority

1. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument not supporting resource priority. Observe that existing call is not preempted.
2. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **routine** to DUT. Observe that existing call is not preempted.
3. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **priority** to DUT. Observe that existing call is not preempted.
4. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **immediate** to DUT. Observe that existing call is not preempted.

5. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash** to DUT. Observe that existing call is not preempted.
6. Place outgoing call with **priority** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash-override** to DUT. Observe that existing call is not preempted.

B.1.8 Test 9: Receive Incoming Call Resource Priority Set to Immediate

1. Place outgoing call with **immediate** resource priority to user off-hook. Place call from end instrument not supporting resource priority. Observe that existing call is not preempted.
2. Place outgoing call wit**h immediate** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **routine** to DUT. Observe that existing call is not preempted.
3. Place outgoing call with **immediate** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **priority** to DUT. Observe that existing call is not preempted.
4. Place outgoing call with **immediate** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **immediate** to DUT. Observe that existing call is not preempted.
5. Place outgoing call with i**mmediate** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash** to DUT. Observe that existing call is preempted.
6. Place outgoing call with **immediate** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to ‘Flash-Override’ to DUT. Observe that existing call is preempted.

B.1.9 Test 10: Receive Incoming Call Resource Priority Set to Flash

1. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument not supporting resource priority. Observe that existing call is not preempted.
2. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **routine** to DUT. Observe that existing call is not preempted.
3. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **priority** to DUT. Observe that existing call is not preempted.
4. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **immediate** to DUT. Observe that existing call is not preempted.

5. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash** to DUT. Observe that existing call is not preempted.
6. Place outgoing call with **flash** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash-override** to DUT. Observe that existing call is preempted.

B.1.10 Test 11: Receive Incoming Call Resource Priority Set to Flash-Override

1. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument not supporting resource priority. Observe that existing call is not preempted.
2. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **routine** to DUT. Observe that existing call is not preempted.
3. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **priority** to DUT. Observe that existing call is not preempted.
4. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **immediate** to DUT. Observe that existing call is not preempted.
5. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to **flash** to DUT. Observe that existing call is not preempted.
6. Place outgoing call with **routine** resource priority to user off-hook. Place call from end instrument supporting resource priority with resource priority set to f**lash-override** to DUT. Observe that existing call is not preempted.

B.1.11 Test 13: Call Forward Test

1. Configure DUT to forward calls to another device as described in Chapter 2, paragraph 2.1.1.1.
2. Place call from different end instrument supporting resource priority with resource priority set to **immediate** to DUT set to forward calls.
3. Observe that resource priority is maintained on forwarded leg of call.

B.1.12 Test 15: Call Transfer Test

1. Place call from different end instrument supporting resource priority with resource priority set to **immediate** to DUT.
2. Configure DUT to transfer call to another device as described in Chapter 2, paragraph 2.1.1.1.

3. Observe that resource priority is maintained on forwarded leg of call.

B.1.13 Test 16: Call Hold Test

1. Place call from different end instrument supporting resource priority with resource priority set to **immediate** to DUT.
2. From DUT, place call on hold.
3. Place call from different end instrument supporting resource priority with resource priority set to **flash** to DUT.
4. Observe that call preemption of the call on hold occurs.
5. Repeat with incoming call of lower priority than call on hold.
6. Observe that call is not preempted.

SYMBOLS, ABBREVIATIONS, AND ACRONYMS

This page intentionally left blank.

3DES	Triple DES
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
3PCC	Third Party Call Control
AAP	Alarm Activation Panel
AC	Access Categories
ACF	Admission Confirm message
ACL	Access Control List
ADC	Analog-To-Digital Converter
ADM	Administrator
ADNS	Automatic Digital Network System
AES	Advanced Encryption Standard
AFE	Analog Front End
AH	Authentication Header
AMR	Adaptive Multi-Rate
AP	Audio Panel
API	Application Programming Interface
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
ARQ	Admission Request message
ASCII	American Standard Code for Information Interchange
ASLAN	Assured Services Local Area Network
ASN	Abstract Syntax Notation
AS-SIP	Assured Services-Session Initiation Protocol
AST	Asynchronous Transfer mode
BISDN	Broadband Integrated Services Digital Network

B2BUA	Back-To-Back User Agent
BOIS	Base Operating Information System
BPSK	Binary Phased Shift Keying
BRI	Basic Rate Interchange
BSD	A family of permissive free software licenses. The original was used for the Berkeley Software Distribution.
BSR	Base Station Router
CA	Certificate Authority
CAAS	Central Amplifier Announcing System
CAG	Carrier Air Group
CALEA	Communications Assistance for Law Enforcement Act
CAM	Content Addressable Memory
CANES	Consolidated Afloat Networks and Enterprise Services
CAS	Common Associated Signaling
CC	Common Criteria
CD	Compact Disc
CDMA	Code Division Media Access
CDP	Cisco Discovery Protocol
CDR	Call Detail Record
CEM	Customer Experience Management
CER	Customer Edge Router
CISSP	Certified Information Systems Security Professional
CIVUT	Compact Integrated Voice User Terminal
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLC	Close Logical Channel
CNG	Comfort Noise Generator
codec	Coder/Decoder
CoS	Class of Service

COTS	Commercial-Off-The-Shelf
CPE	Customer Premises Equipment
CPIM	Common Presence and Instant Messaging
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSMA	Carrier Sensed Multiple Access
CT	Connecticut
CVN	Nuclear-Powered Attack Submarine
DAC	Digital-To-Analog Converter
DARPA	Defense Advanced Research Projects Agency
DARTS	DISN Assured RTS Support
DCF	Disengage Confirm
DDG	Guided Missile Destroyer
DDRE	Dual-Decision Feedback Equalizer
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dial
DISA	Defense Information System Agency
DNS	Domain Name Service
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense
DoDI	DOD Instruction
DoS	Denial of Service
DRM	Digital Rights Management
DRQ	Disengage Request
DRSN	Defense Red Switch Network
DS	Dedicated Station

DSA	Digital Signature Algorithm
DSN	Defense Switched Network
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
DT	Dial Telephone
DTMF	Dual-Tone Multi-Frequency
DTP	Dynamic Trunking Protocol
DUT	Device Under Test
DVD	Digital Versatile Disc
DVMRP	Distance Vector Multicast Routing Protocol
DVX	Deployable Voice Exchange
EAL	Evaluated Assurance Level
EBC	Edge Boundary Controller
E&M	Ear and Mouth
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol -Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol -Tunneled Transport Layer Security
EAPOL	Extensible Authentication Protocol Over LAN
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECAS	Electronic Call Accounting System
ECS	Exterior Communications System
EI	End Instrument
EIA	Electronic Industries Association
E&M	Ear and Mouth
EMCON	Emission Controls
EO	End Office
EPCC	End-Point Call Control
ESC	End Session Command

ESP	Encapsulated Security Payload
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standards
FSB	Fleet Select Box
FTP	File Transfer Protocol
FXS	Foreign Exchange Station
GA	General Alarm
GARP	Gratuitous Address Resolution Protocol
GCCS	Global Command and Control System
GIG	Global Information Grid
GigE	Gigabit Ethernet
GIPS	Global IP Solutions Inc.
GMSK	Gaussian Minimum Shift Keying
GPHY	Gigabit Physical
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile
GSTN	General Switched Telephone Network
GUI	Graphical User Interface
HA	High Availability
HAIPE	High Assurance Internet Protocol Encryptor
HMAC	Hashed Message Authentication Code
HPI	Host Port Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
IA	Information Assurance

iAC	Intelligent Advanced Communications
iACT	Intelligent Advanced Communications Terminal
IANA	Internet Assigned Numbers Authority
IAX	Inter-Asterisk Exchange Protocol
IC	Integrated Communication
ICAN	Integrated Communications and Advanced Networks
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for Ipv6
ICS	Integrated Communications System
ICSAP	Integrated Communications System Audio Panel
ICSCU	ICS Control Unit
ICT	Integrated Communication Terminal
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
iLBC	internet Low Bitrate Codec
IM	Instant Messaging
IOM	ISDN-Oriented Modular
IP	Internet Protocol; Inter-Phone
IPDC	IP Device Control
IP-PBX	IP-Public Branch Exchange
IPSec	IP Security
IS	Intrinsically Safe
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IVCN	Integrated Voice Communications Network
IVN	Integrated Voice Network
IVUT	Integrated Voice User Terminal
JITC	Joint Interoperability Test Command
JTAG	Joint Test Action Group
LAN	Local Area Network
LATA	Local Access and Transport
LCD	Liquid Crystal Display
LCS	Littoral Combat Ship
LEAP	Lightweight Extensible Authentication Protocol
LGS	LGS Innovations, LLC, Subsidiary of Alcatel-Lucent
LLC	Logical Link Control; Limited Liability Company
LMR	Land Mobile Radio
LSC	Local Session Controller
LSP	Label-Switch Path
LSSGR	Local Switching Systems Generic Requirements
LTE	Long Term Evolution
LTIU	Lockout Trunk Interface Unit
MAC	Media Access Control
Mbps	Megabit Per Second
MC	Multi-Channel
MCU	Multipoint Control Units
MFS	Multifunction Switch
MG	Media Gateway
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIKEY	Multimedia Internet Keying

MIME	Multipurpose Internet Mail Extensions
MIMO	Multiple-Input/Multiple-Output
MIPS	Microprocessor without Interlocked Pipeline Stages
MitM	Man in the Middle Attacks
MLPP	Multi-Level Precedence and Preemption
MMU	Memory Management Unit
MMUSIC	Multiparty Multimedia Session Control
MOS	Mean Opinion Score
MPLS	Multi Protocol Label Switching
MSTP	Multiple Spanning Tree Protocol
MWS	MORIAH Wind System
NAPT	Network Address Port Translation
NAT	Network Address Translators
NAVSSI	Navigation Sensor System Interface
NIC	Network Interface Card
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NLOS	Near Line of Sight
NMS	Network Management System
NSA	National Security Agency
NVP	Network Voice Protocol
OAMP	Operations, Administration, Maintenance, And Provisioning
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Media Access
OLC	Open Logical Channel
OMA	Open Mobile Alliance

ONR	Office of Naval Research
OOB	Out-Of-Band
OOP	Object Oriented Programming
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PA	Public Address; Presence Agents
PAgP	Port Aggregation Protocol
PAN	Personal Area Network
PBX	Private Branch Exchange
PBX1	Private Branch Exchange Type 1
PBX2	Private Branch Exchange Type 2
PC	Personal Computer
PCAP	Packet Capture
PCM	Pulse-Code Modulation
PDA	Personal Digital Assistant
PER	Pack Encoding Rules
PHY	Generic electronics term referring to a special electronic integrated circuit or functional block of a circuit that takes care of encoding and decoding between a pure digital domain (on-off) and a modulation in the analog domain.
PICT	Programmable Integrated Communication Terminal
PKI	Public Key Infrastructures
PoC	Proof-of-Concept
PoE	Power Over Ethernet
POT	Plain Old Telephone
PP	Protection Profile
PRACK	Provisional Response Acknowledgement
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network

PTT	Push-To-Talk
PUA	Presence User Agent
PVST	Per VLAN Spanning Tree
QAM-16	Quadrature Amplitude Modulation-16
QAM-64	Quadrature Amplitude Modulation-64
QoS	Quality of Service
QPSK	Quadrature Phased Shift Keying
R&D	Research and Development
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Drives
RAM	Random Access Memory
RAS	Register, Admission, Status protocol
RCCS	Ruggedized Command & Control Solutions
RCS	Radio Communication System
RF	Radio Frequency
RFC	Request For Comments
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RMII	Reduced Media Independent Interface
RPR	Resilient Packet Ring
RSA	Rivest, Shamir, Adleman
RSSE	Reduced-State Sequence Estimator
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
RTCP	Real-Time Control Protocol
RTS	Real Time Services
SA	Security Association

SATCC	Ship Air Traffic Control Communications
SBC	Single Board Computer; Session Border Controller
SBU	Secure But Unclassified
SCCP	Skinny Client Control Protocol
SCD	Source Control Drawing
SCDS	Ships Control Display System
SCN	Switch Circuit Network
SCSI	Small Computer System Interface
SDK	Software Development Kits
SDP	Session Description Protocol
SDRAM	Synchronous Dynamic Random Access Memory
SES	SIP Enablement Server - Avaya
SGCP	Simple Gateway Control Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SISO	Single-Input/Single-Output
SMEO	Small End Office
S/MIME	Secure / Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SNAC	Systems and Network Attack Center
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol; Service Oriented Architecture Protocol
SPAN	Switched Port Analyzer
SPAWAR	Space and Naval Warfare Systems Command
SPI	Serial Peripheral Interface Bus
SPIT	Spam Over Internet Telephony
SPT	Sound Powered Telephone; Sound Powered Telephony
SRTP	Secure Real-time Transport Protocol

SSL	Secure Socket Layer
SS7	System Signaling #7
SSN	Fast Attack Submarine
STE	Secure Telephone Equipment; Secure Terminal Equipment
STIG	Security Technical Implementation Guide
STP	Spanning Tree Protocol
STU	Secure Terminal Units
STUN	Simple Traversal of UDP Through NATs
SVP	SpectraLink Voice Priority
T1	Digital signal 1 (also known as DS1) is a T-carrier signaling scheme widely used in telecommunications in North America and Japan to transmit voice and data between devices.
TCP	Transmission Control Protocol
TCS	Terminal Capability Set
TDM	Time-Division Multiplexing
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TI	Texas Instruments
TIA	Telecommunications Industry Association
TLB	Translation Lookaside Buffer
TLS	Transport Layer Security
ToS	Type of Service
TRP	Transport, Routing and Package
TSCE	Total Ship Computing Environment
TTL	Time to Live
TURN	Traversal Using Relay NAT
TVS	Tactical Variant Switch
Tx/Rx	Transmit/Receive
UA	User Agent; Universal Alcatel

UAC	User Agent Client
UART	Universal Asynchronous Receiver/Transmitter
UAS	User Agent Server
UCR	Unified Capabilities Requirements 2008
UDDI	Universal Description, Discovery and Integration
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UMB	Ultra Mobile Broadband
UMTS	Universal Mobile Telecommunication System
UNISTIM	Unified Networks IP Stimulus
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States
USB	Universal Serial Bus
UWB	Ultra-Wide Band
VLAN	Virtual Local Area Networks
VLYNQ	Proprietary interface developed by Texas Instruments
VM	Voice Mail
VMPS	VLAN Management Policy Server
VoIP	Voice Over Internet Protocol
VOMIT	Voice Over Misconfigured Internet Telephones
VOX	Voice Operated Switch
VPN	Virtual Private Network
VQP	VMPS Query Protocol
VRRP	Virtual Router Redundancy Protocol
VTP	VLAN Trunking Protocol
VWCS	Virtually Wirefree Communications System
VXML	Voice eXtensible Markup Language
WAN	Wide Area Network

WEP	Wired Equivalent Privacy or Wireless Encryption Protocol
WIFCOM	Wire Free Communication
Wi-Fi	"Wireless Fidelity". Generically used to describe wireless interface of mobile computing devices, such as laptops in LANs. Wi-Fi® and the Wi-Fi CERTIFIED™ logo are registered trademarks of the Wi-Fi Alliance®.
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WME	Wireless Multimedia Extensions
WMM	Wi-Fi Multimedia
WPA/ WPA2	Wi-Fi Protected Access
WSDL	Web Services Description Language
XML	Extensible Markup Language